Vehicle to Everything (V2X) : An Overview

Akshita Jakhar
Computer Science and Engineering
(School of Engineering)
Shiv Nadar Institution of Eminence
Greater Noida, India
aj232@snu.edu.in

Shrey Sharma
Computer Science and Engineering
(School of Engineering)
Shiv Nadar Institution of Eminence
Greater Noida, India
ss989@snu.edu.in

***Abstract*— We are aiming for a truly intelligent transportation system capable of providing novel user-experience while significantly increasing road safety, traffic efficiency, improving air quality, and providing a plethora of cutting-edge applications. A considerably improved vehicle-to-everything (V2X) communication network that can simultaneously support rapid, highly-reliable, and low-latency information exchange at a massive scale is necessary to realise this ultimate goal. Due to the growing urbanization and technological advancements the issues of data security, traffic safety, and capacity limits are brought to light with regard to V2X. This article focuses on development of V2X over the years and the benefits and challenges faced. It includes the research work in the field of 5G and 6G. To encourage further studies, we have addressed the open challenges, future work and possible applications.**

Keywords*— *Vehicle-to-Eveyrthing V2X, 5G, application, requirements, 6G, 3GPP, challenges

I. INTRODUCTION

V2X is a key enabler for intelligent transportation systems (ITSs), which comprises of a broad range of wireless technologies - vehicle-to-vehicle (V2V) communications, vehicle-to-infrastructure (V2I) communications, and vehicle-to-pedestrian (V2P) communications, communications with vulnerable road users (VRUs) and with cloud networks (V2N) [1]. The adoption of this technology is responsible for linking the various transportation elements like roads, vehicles, pedestrians and cloud environments, which will result in increasing traffic efficiency, lowering pollution, saving resources, lowering the frequency of accidents, and better traffic management, in addition to a plethora of advanced applications [2]. Till now, there have been two primary technical methods of V2X communication: 1) Dedicated short-range communication (DSRC)-based vehicular network and 2) cellular-based vehicular network. We will discuss these in the following sections. Electronic control units, an embedded computing platform used to monitor and control automotive systems, are linked with sensors and actuators to form the internal architecture of a car. External interfaces are used for the vehicle's communication with the outside world, such as other vehicles or roadside units (RSUs). These vehicle external connections are connected to the onboard unit (OBU), also known as the telematics control unit (TCU), an ECU that offers wireless connectivity [3].

The paper discusses the background of V2X communication with DSRC and 3GPP releases, followed by its use cases, applications, current network challenges, open challenges and future work in the field of 6G.

A. DSRC

Standards that form the backbone of DSRC include IEEE 802.11p for Wireless Access in Vehicular Environments (WAVE) at the physical layer and Medium Access Control (MAC) layer, which simplifies authentication, associated processes, and data transmission before sending data, enabling vehicles to broadcast relevant security information directly to neighbouring vehicles and pedestrians and IEEE 1609.1.4 for resource management, security, network service, and multichannel Operation. At the application layer, SAE J2735 defines the message format used for communication, and the J2945/x family of standards defines various scenarios [2]. The only viable technology for V2X transmission for many years was DSRC. However, it suffered from major drawbacks, such as limited coverage, low data rate, limited quality-of-service (QoS) guarantees, and unbounded channel access delay [1].

B. 3GPP Releases

3GPP Release 14 proposed LTE V2X communication with two air interfaces: a wide area network LTE interface (LTE-Uu) and a direct communications interface (PC5, also known as LTE side-link). The LTE-Uu is responsible for vehicle-to-network (V2N) communication, while the LTE side-link is responsible for V2V and V2I communications, which may operate without support from the cellular network infrastructure [1]. The Uu mode uses the existing LTE cellular network to implement V2V communication by forwarding, and the PC5 mode is similar to the DSRC, enabling direct communication between vehicles. Additionally, the PC5 interface has been enhanced in many aspects to accommodate exchanges of rapidly changing dynamic information (position, speed, driving direction, etc.) and future advanced V2X services (automatic driving, vehicle platooning, sensor sharing, etc.) [2]. To enable advanced V2X services like vehicle platooning, advanced driver assistance, remote driving, and extended sensors, 5G New Radio (5G NR) V2X technology was launched in Release 15. Additionally, while maintaining backward compatibility with Release 14 LTE-V2X, the performance of the PC5 interface has been improved in Release 15 in terms of greater reliability, reduced latency, and higher data rates. The second phase of 5G NR, which seeks to bring improved ultrareliable low-latency communication (URLLC) and higher throughput, was announced by 3GPP in Release 16 in 2020. Release 17 of the 3GPP is presently under development and seeks to offer architectural improvements to support advanced V2X services[1].

C. Use Cases

Computing, storage, and virtual network functions are placed at the edge of the access network to support V2X services, such as road surface ice detection, video and map sharing, and vehicle platooning, that require low latency or location awareness. Use cases of V2X can be divided into the following few categories[4-5]:

- Cooperative Awareness: V2V/V2I communication helps vehicles understand their surroundings and provide emergency vehicle warnings.
- Cooperative Sensing: Cooperative autonomous driving is based on V2V/V2I communications to improve sensor data and objective information from radars.
- Cooperative Manoeuvring: V2V- / V2I - based cooperative manoeuvring enables autonomous vehicles to coordinate decision-making.
- Awareness of VRUs: VRUs refer to road users with high casualty rates.
- Improving Traffic Efficiency: V2I and V2N communications are not delay-sensitive but can help improve traffic efficiency.
- Tele-operated Driving: Tele-operated driving uses V2N communications to control a vehicle in normal traffic remotely.

II. APPLICATIONS

Numerous sectors and cross-industry alliances have studied the requirements for V2X business applications and are working towards them. The current applications can be categorized into three: 1)Safety Applications which involve collision warnings, road hazard warnings, speeding warnings, and anything related to personal safety, the safety of the vehicle, or the safety of pedestrians. 2) Efficiency Applications help drivers travel more safely and efficiently by providing congestion warnings and green wave speed guidance. 3) Information services applications refer to software tools like eCall, traffic information and route suggestions, and automatic parking that give owners access to vehicle-related information to enhance navigation. 3GPP has defined four types of advanced application scenarios: Vehicle Platooning, Advanced Driving, Extended Sensors, and Remote Driving. Entertainment services are also expected to join the V2X industry soon. These applications are being developed keeping in mind that latency/reliability requirements and safety requirements take the topmost priority [2].

III. NETWORK CHALLENGES

With the advent of V2X came multiple issues regarding reliability, network congestion, data transmission due to continuously changing topology and high mobility, and concerns about privacy, security, and trust. This section highlights the challenges and the strategies to deal with them. V2X security approaches can be divided into two classes: entity-centric and data-centric. Entity-centric approaches focus on identifying the misbehaving node based on trust establishment, while data-centric approaches verify the correctness of the received data. Entity-centric detection approaches can be further subdivided into behavioural (e.g., observing patterns in the behaviour of specific nodes at the protocol level) and trust-based. Data-centric mechanisms are similar to intrusion detection in traditional computing systems and can be either plausibility-based (model-based approach that verifies if the information transmitted from a particular sender is consistent with the model) or consistency-based. Depending on the scope, detection mechanisms can be local, cooperative, or hybrid. Behavioural and plausibility schemes operate locally and rely on cooperation among vehicles/RSUs to detect inconsistencies, while consistency-based mechanisms can also be performed locally for more fine-grained detection.

A. Latency/Reliability

1) Challenges

For V2X networks and its applications to function fluently, we need to have low latency and high reliability. DSRC is known to achieve this combination of low latency and high reliability using CSMA/CA for non-dense vehicle environments; however, it fails otherwise. LTE-V2X has relatively stable latency, but it faces different types of attacks like jamming attacks and greedy behaviour attacks (DoS), which reduces the performance by exhausting the network resources. 5G networks provide a communication delay of less than 1 ms while providing stability of 99.999% so that they will be able to support automatic-driving-oriented V2X services. 6G networks will take it one step further by providing ultrafast and super-efficient network performances for a dense network.

2) Testing: Testing is an indispensable part of Internet of Vehicles. It ensures the reliability of communication which results in the safety of the entire V2X environment. Function testing, performance testing, and communication protocol conformance testing are mainly used to meet the testing requirements for latency and reliability. Security protocol consistency, gateway testing, penetration testing, and accelerated testing can find vulnerabilities and potential risks and its applications to ensure its security.

- *Conformance Testing* ensures interoperability between vehicles, pedestrians, RSU, cloud platform, and other participants, which is the basis for developing various types of V2X applications. It has two sub-parts: Communication Protocol, meant for stipulating the data format and interaction flow of processes and Security Protocol, meant for stipulating certification and authentication.
- *Function testing* is used to test for rapid action and response time for a particular trigger. Laboratory testing is used to simulate real-life scenarios and test the network without spending loads of money and time. Field testing is used as well as virtual testing has its limitations and can't accurately reflect objective facts.
- *Performance testing* is done to guarantee the latency and reliability requirements of V2X applications. It includes end-to-end communication delay testing, packet delivery success rate testing, and parameter testing.
- *Vehicle Gateway Testing*: The architecture consists of two parts: the system under test and the test system. According to test cases, the test system inputs the test data to the system under test, which

generates the corresponding response according to the input of the test system. The test system conducts tests by analysing the differences between the expected results and the actual results obtained from the system under test.

- *Penetration testing* is meant to test the security of the system by mimicking an attacker's methods. It is divided into three categories – White box testing: when testers are given information like design specifications, code implementation, etc. of the system in advance. Black box testing: Testers have no information in advance; it is more realistic. Grey box testing: It is a mix of black box and white box testing. Interface testing, transportation testing, and system testing are the three different kinds of specialised penetration testing. Interface testing focuses on those between cars, mobile devices, and roadside equipment. Transportation testing centres on problems with misuse, poor communication protocol design, and ineffective cryptographic schemes. System testing looks at implementation defects, insecure system settings, and other known weaknesses of the cloud systems, mobile terminal OSs, vehicle gateways, and other systems.
- *Accelerated testing* requires tons of real-world data and critical scenarios to analyse potential problems and give results while cutting the cost and time spent on the verification process.
- *Field testing* requires a large number of basic network facilities and transportation facilities, test vehicles, testers, etc. To reduce the cost of this process, Parallel testing is used.

B. Trust

1) Challenges: Trust management is essential for developing secure V2X services, as hackers can exploit network devices and system failures can occur. To ensure trust in 5G V2X architecture, all system entities must register their real identities through a trust authority (TA), which issues, stores, and revokes certificates (such as certified public keys). However, it is important to note that a certificate can only verify a registered entity's ownership of a public key, and the entity's trustworthiness cannot be fully guaranteed. Thus, in addition to certificate-based trust strategies, other strategies, such as reputation-based trust strategies, should also be jointly considered.

Bad Mouth Attacks, Conflicting Behavior Attacks, Blackhole Attacks, Sybil Attacks, and On-Off Attacks are all types of DoS attacks that can undermine trustworthiness between entities. Bad Mouth attacks involve falsely promoting malicious entities or discrediting good ones. Conflicting behaviours can occur between two different entity groups, while Blackhole Attacks involve discarding packets that should be relayed. Sybil Attacks involve forging fake identities to take the blame for bad behaviour patterns.

2) Strategies: We review the trust management strategies proposed for each layer of 5G V2X systems' layered paradigm., as follows-

- *Trust Management Strategies in Data Networks/Internet:*A V2X service requires user authentication from the start, which is done through X.509 certification. Trusted certificates are issued by a certification authority (CA) and can be revoked for expired or compromised entities using a certificate revocation list (CRL). Trust in mobile social communications can be established centrally or locally using cellular or DSRC technologies. Direct trust is propagated to neighbour entities based on topology- and evidence-based methods, with action and recommendation trust scores, maintained separately to defend against trust attacks.

- *Trust Management Strategies in 5G Core Networks:* 5G core networks use strong cryptographic primitives to increase trust between communicating entities. Instead of physical USIM cards, certificates, pre-shared keys, and token cards are allowed in 5G AKA protocols and EAP framework. New technologies such as SDN and NFV improve the trustworthiness of 5G core networks by enhancing system resilience and network slicing.

- *Trust Management Strategies at Network Edge:* Edge servers owned by different providers allow for finer-grained trust from users. Trusted certificates should authenticate edge servers and users, and authentication policies should consider location and resource ownership. Trustworthy edge servers can coexist with malicious ones in distributed edge server overlays. Research has been conducted on distributed trust evaluation and management based on blockchain technology, which removes the need for trust in a central party and ensures reliable data management.

C. Security

1) Challenges: 5G V2X services must meet basic security requirements such as confidentiality, authenticity, integrity, and availability to ensure authorized users can access the services. Security attacks in 5gV2X include eavesdropping, message forgery, jamming, impersonation, replay attacks, and Sybil attacks. Eavesdropping is possible due to the broadcast nature of wireless communication, while message forgery and jamming are caused by false messages or false warnings. Impersonation is used to gain/forge the credentials of other legitimate vehicles, while replay attacks are used to disrupt the traffic flow. Sybil attacks involve generating multiple identities and using each identity to send different messages to other vehicles. MITM attacks involve sniffing any exchanged information between two V2X communication entities and attempting to impersonate one of them. These attacks can lead to the loss of property and human lives on the road.

Attacks on Network Edge include location spoofing, DoS attacks, fake attacks, and saturation attacks. Edge servers are more vulnerable to DoS attacks due to their resource-restricted nature, while 5G Core Networks are vulnerable to Hijacking attacks, which exploit the vulnerability of SDNs.

Saturation attacks are when an attacker crafts an inbound stream of flow requests to make 5G V2X services unavailable. OpenFlow controllers use Link Layer Discovery Protocol (LLDP) packets to discover links among OpenFlow switches, making them vulnerable to link fabrication attacks and unauthorized slice access attacks. To achieve authorized network slice access, isolation is necessary.

2) Strategies:

- *Security Strategies in Data Networks/Internet:* Before DoS attacks, techniques can be applied to prevent malicious traffic, such as anomaly and signature-based detection. During the attacks, machine learning-based detection techniques can be used to detect the DoS attacks by checking whether the rate of flow of the packets reaches a given threshold or not, finding out anomalies inside the packets, and comparing them with the normal behaviour of the packets using machine learning.

- *Security Strategies in 5G Core Networks*:5G core is affected by some of the vulnerabilities in SDN and NFV since these techniques are two of its building blocks. We classify host location hijacking attacks and link fabrication attacks as topology poisoning attacks, which can be effective due to the lack of validation of the packets and APIs used for topology management. To mitigate these attacks, TopoGuard, a security extension for the OpenFlow controller, is proposed. TopoGuard uses a port manager to maintain properties indicating the state of each switch port and will raise an alert when an illegal action corresponding to the current state happens. We also propose an extension called connection migration to reduce the amount of data-to-control-plane interactions.

- *Security Strategies in V2X Communications:* Eavesdropping attacks are passive attacks that cannot be easily traced, and encryption is a common technique to counter them. Friendly jamming is a promising approach to prevent eavesdropping attacks without bringing extra computing tasks. To prevent an impersonation attack, all messages should be authenticated and signed, such as user authentication using a digital signature, employing a TA, and using variable MAC and IP addresses. To address replay attacks, two strategies can be used: a globally synchronized time for all V2X entities and a nonce (timestamp) attached to the messages. MITM attacks are when a malicious V2X entity listens to communication and injects false information, while Sybil attacks are when an attacker generates multiple identities to take the wrong action.

D. Privacy

1) Strategies:

- *Privacy Strategies in Data Networks/Internet:* Anonymous credential enables users to access V2X services without exposing real identities. It can be constructed using blind signatures, group signatures, or pseudonyms. Combining blind signature and secret sharing scheme to design a privacy-preserving scheme to protect vehicle's privacy while still offering an effective way to discover traffic law violators. The blind-signature-based anonymous credential has two desirable features: it can be used multiple times for service access, and the user's identity is perfectly preserved.
- *Privacy Strategies in 5G Core Networks:* Pseudonyms are assigned by network operators to vehicles as permanent identifiers to ensure identifier privacy and secure exchange of V2X messages. AnonyFlow is an efficient SDN-based anonymization service where the Internet users offload trust to the primary service providers that assign temporary IP addresses and disposable flow-based identifiers to users.
- *Privacy Strategies at Network Edge:* Encryption and pseudonym-based schemes are used to protect against eavesdropping in the edge layer. Differential privacy using mathematical noise is an effective way to achieve location privacy in location-based services, but it can lead to inaccurate location information.
- *Privacy Strategies in V2X Communications:* Mix networks use proxy servers to shuffle messages from multi-senders and return back at random to prevent adversarial tracing. MixGroup allows vehicles to exchange pseudonyms at extended pseudonym-changing areas, increasing the uncertainty of the pseudonym mixture. Pseudonym-based approaches to secure vehicular communications include randomizing public-key certificates to generate key pairs or symmetric cryptography by randomly choosing pseudo identities. SCMS is the leading candidate for secure communication in the US, and identity-based cryptography is used to generate and issue pseudonyms. To remove the dependence on TA, roadside infrastructures are allowed to issue pseudonyms, and threshold-based secret sharing schemes are used to collaboratively generate the secret key of the vehicle from the pseudonym and reveal the vehicle's identity in the presence of k out of n authorities.

IV. INTEGRITY CHECKING

The integrity of V2X communication can be verified from different contexts such as -

A. Event Validation

We propose a message filtering mechanism that combines parameters of messages into a single entity called the 'certainty of event' (CoE) curve. CoE is calculated by combining data from various sources, such as local sensors and RSUs, and using consensus mechanisms (e.g., messages from other vehicles and validation by infrastructure). Message validity is defined using a threshold curve, and false positives for events can be reduced when more evidence is obtained over time. Researchers also proposed to determine the correctness of event reports through voting and post-event detection.

B. Behavioral Analysis and Message Integrity Checking

The VEBAS (vehicle behaviour analysis and evaluation scheme) protocol allows the detection of unusual vehicle behaviour by analyzing all messages received from neighbouring vehicles. The MisDis protocol ensures accountability of vehicle behaviour by recording all the (sent/received) messages for each vehicle peer in a secure log. A plausibility validation network (PVN) to protect the V2X applications from false data injection attacks has also been proposed. The PVN uses a rule database and a checking module to check the plausibility of the received messages. A limitation of this approach is that since the rule database is shared, a malicious vehicle can generate valid messages to avoid detection.

C. Location and GPS Verification

HASAN et al. proposed to secure vehicle-to-everything (V2X) communication platforms by using two verifiers: acceptors (distributed over the region) and rejecters (placed around acceptors in a circular fashion). If the message is first received by the acceptors, then they will verify that the vehicle is within the region, but a malicious vehicle can spoof its location when it resides within the region. Another way is to use onboard radar to detect the physical presence of vehicles (e.g., which vehicles are in proximity) with GPS information received from other vehicles to isolate malicious nodes. This mechanism can prevent some variants of Sybil attacks.

An attacker can send delayed responses to each RSU, so an alternative trust-based verification approach is proposed where a vehicle discards packets if the included position information is further than the predefined maximum acceptance range threshold. Similar ideas can be used by exchanging position beacons among neighbours, which can be improved by ignoring further beacons when too many are sent from one area, map-based verification, and position claim overhearing. However, these checks may not perform well individually.

D. Reputation Analysis and Revocation

We use statistical techniques to predict and explain traffic flow and determine whether or not a sender is malicious. Bayesian logic has been proposed to compute the 'probability of maliciousness' of a vehicle for a time t. The T-VNets framework evaluates two trust parameters: inter-vehicle trust (e.g., by combining data-centric evaluation of messages received from each neighbour) and RSUs-to-vehicles. Raya et al. proposed LEAVE (local eviction of attackers by voting evaluators) to detect which neighbour differentiates from other neighbours. Moore et al. (called Stinger) proposed a similar idea in which both the reporting as well as reported vehicles are temporarily prohibited from sending messages. Both LEAVE, and Stinger protocols require an honest majority, as too many compromised neighbours could present malicious behaviours as normal.Direct communication between two vehicles mainly use: a)Network assistance communication and b)Autonomous direct communication. Network assistance communication is the centralized system of LTE for supporting V2V direct communications, while autonomous direct communication is proposed for V2V communications in a decentralized architecture.

V. PERFORMANCE EVALUATION

Simulation results show that network assistance communication has an advantage in freeway and urban environments. Performance metrics such as Packet Reception Rate (PRR) and Delay are used to measure transmission reliability. PRR is the ratio that the transmitted message can be successfully decoded by the receiving mode at the specific distance, while Delay is the time difference between the time of transmitting and receiving the V2X service packet.

Simulation –

The vehicles appear as Poisson distribution and the speed follows a Gaussian distribution with the given mean values depending on the lane. WINNER + B1 channel model is selected as the channel model with the distance between transmitter and receiver.

Public parameter	Assumptions
Bandwidth	10MHZ
Carrier frequency	5.9GHz
Transmitted power	23 dBm
Antenna configuration	1 TX and 2 RX
Antenna pattern	Omni
Antenna gain	3 dB
Modulation	QPSK, code rate ~=1/2
Lane	6(3 in each direction)
In-band emission	{3,6,3,3}
Communication type	broadcast

Table I. Parameter simulations parameter

Freeway scene parameter 1	Assumptions
Freeway length	6900m
Width of Lane	3.5m
Vehicle density for 1km	60vehicles
Inter-site distance	1725m
Vehicular mobility model	Gaussian distributed, mean values of speed are 23m/s,30m/s and 37 m/s from center to side, standard deviation is 1m/s.

Table II. Freeway scene 1 simulations parameter

Freeway scene parameter 2	Assumptions
Freeway length	2400m
Width of lane	3.75m
Speed	Uniform distributed, from inner lane to outside lane:(100,200), (80,100),(60,80)
Mean inter-arrival time (from inner lane to outside lane)	2.7s,4.4s,7.1s ,2.0s,3.2s,5.1s
Inter-site distance	1200m

Table III. Freeway scene 2 simulations parameter

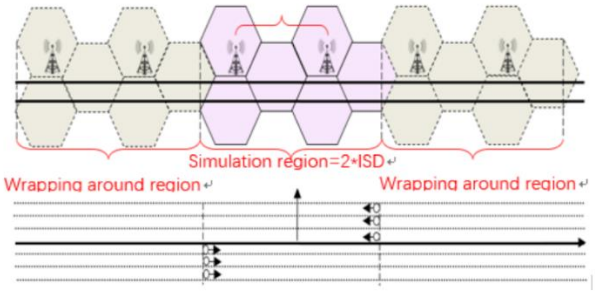

Fig. 1. Simulation zone is mapped into wraproud in freeway scene

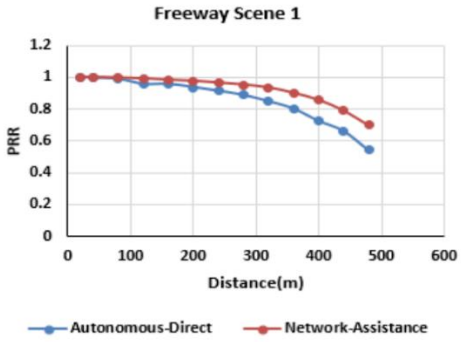

Fig. 2. PRR of autonomous-direct communication and network-assistance communication in freeway scene 1

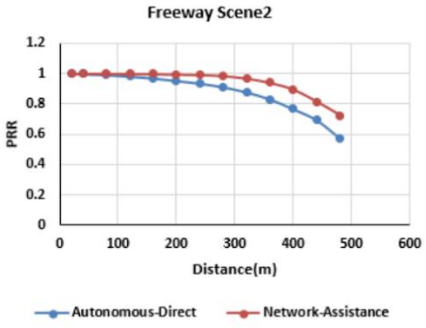

Fig. 3. PRR of autonomous-direct communication and network-assistance communication in freeway scene 2

The performance of network assistance communication and autonomous direct communication in freeway scenes 1 and 2 is mainly focused on the communication radius of 320m between the transmitting vehicle and receiving vehicle. The diagram clearly shows that network assistance communication is better than autonomous direct communication, and the performance gain is more obvious with increasing distance, up to 15% in fig.2 and fig.3.

VI. 6G V2X

There is a range of key technologies that we might enable the future vision of 6G-V2X as an intelligent, autonomous, user-driven connectivity and service platform for ITS. We classify these technologies into *revolutionary* V2X technologies and *evolutionary* V2X technologies. They have been summarized in the table [1].

VII. Open Problems

1) Secure Network Caching at Network Edge Caching data at storage spaces on edge devices is an effective way to reduce latency, but it is difficult to ensure confidentiality. To secure network caching, cache placement strategies, data replacement approaches, and secure data retrieval schemes should be investigated.

2) Security-Enhanced Network Slicing The key security issue is how to perform access authentication and authorization for a specific network slice, which requires additional authentication and authorization to prevent unauthorized vehicles from accessing the slices and ensure low-latency V2X service access.

References

[1] M. Noor-A-Rahim et al., "6G for Vehicle-to-Everything (V2X) Communications: Enabling Technologies, Challenges, and Opportunities," in Proceedings of the IEEE, vol. 110, no. 6, pp. 712-734, June 2022, doi: 10.1109/JPROC.2022.3173031.

[2] A survey of Vehicle Everything(V2X) testing, Jian Wang, Yameng Shao, Yuming Ge.

[3] Securing_Vehicle-to-Everything_V2X_Communication_Platforms.

[4] M. Boban, A. Kousaridas, K. Manolakis, J. Eichinger and W. Xu, "Connected Roads of the Future: Use Cases, Requirements, and Design Considerations for Vehicle-to-Everything Communications," in IEEE Vehicular Technology Magazine, vol. 13, no. 3, pp. 110-123, Sept. 2018, doi: 10.1109/MVT.2017.2777259.

[5] R. Lu, L. Zhang, J. Ni and Y. Fang, "5G Vehicle-to-Everything Services: Gearing Up for Security and Privacy," in Proceedings of the IEEE, vol. 108, no. 2, pp. 373-389, Feb. 2020, doi: 10.1109/JPROC.2019.2948302.

[6] Y. Hu, J. Feng and W. Chen, "A LTE-Cellular-Based V2X Solution to Future Vehicular Network," 2018 2nd IEEE Advanced Information Management,Communicates,Electronic and Automation Control Conference (IMCEC), Xi'an, China, 2018, pp. 2658-2662, doi: 10.1109/IMCEC.2018.8469236.

[7] K. Zaidi, M. B. Milojevic, V. Rakocevic, A. Nallanathan, and M. Rajara- jan, “Host-based intrusion detection for VANETs: A statistical approach to rogue node detection,” IEEE Trans. Veh. Technol., vol. 65, no. 8, pp. 6703–6714, Aug. 2016.