


Review

A Survey of Vehicle to Everything (V2X) Testing

Jian Wang ^{1,2,*} , Yameng Shao ^{1,2}, Yuming Ge ³ and Rundong Yu ³

¹ College of Computer Science and Technology, Jilin University, Changchun 130012, China; shaoyameng@hotmail.com

² Key Laboratory of Symbolic Computation and Knowledge Engineering of Ministry of Education, Jilin University, Changchun 130012, China

³ Technology and Standards Research Institute, China Academy of Information and Communications Technology, Beijing 100191, China; geyuming@caict.ac.cn (Y.G.); yurundong@caict.ac.cn (R.Y.)

* Correspondence: wangjian591@jlu.edu.cn; Tel.: +86-431-85159419; Fax: +86-431-85168337

Received: 17 December 2018; Accepted: 11 January 2019; Published: 15 January 2019



Abstract: Vehicle to everything (V2X) is a new generation of information and communication technologies that connect vehicles to everything. It not only creates a more comfortable and safer transportation environment, but also has much significance for improving traffic efficiency, and reducing pollution and accident rates. At present, the technology is still in the exploratory stage, and the problems of traffic safety and information security brought about by V2X applications have not yet been fully evaluated. Prior to marketization, we must ensure the reliability and maturity of the technology, which must be rigorously tested and verified. Therefore, testing is an important part of V2X technology. This article focuses on the V2X application requirements and its challenges, the need of testing. Then we also investigate and summarize the testing methods for V2X in the communication process and describe them in detail from the architectural perspective. In addition, we have proposed an end-to-end testing system combining virtual and real environments which can undertake the test task of the full protocol stack.

Keywords: V2X; V2X testing; applications; requirements

1. Introduction

The vehicle to everything (V2X) concept uses the latest generation of information and communication technology to realize omnidirectional vehicle to vehicle (V2V), vehicle to infrastructure (V2I), vehicle to pedestrian (V2P), and vehicle to network/cloud (V2N/V2C) network connections [1]. This technology links the various elements of transportation, such as pedestrians, vehicles, roads, and cloud environments. V2X not only can support vehicles to help them obtain more information and promote the innovation and application of automated driving technology, but also can contribute to building an intelligent transport system and promote the development of new modes and new forms of automobiles and transportation services [2]. It is of great significance for improving traffic efficiency, reducing pollution [3], saving resources, reducing the incidence of accidents, and improving traffic management [4].

Currently, there are two main types of communication technologies used for V2X: Dedicated Short Range Communication (DSRC) and Long Term Evolution for V2X (LTE-V2X). The DSRC system consists of a series of IEEE and SAE standards [5]. At the physical layer and the medium access control (MAC) layer, DSRC uses the 802.11p protocol [6], which simplifies authentication, associated processes, and data transmission before sending data, enabling vehicles to broadcast relevant security information directly to neighboring vehicles and pedestrians. The network architecture and security protocols are defined in IEEE 1609 WAVE [7–9]. At the application layer, SAE J2735 [10] defines the message format used for communication, and the J2945/x family of standards defines various scenarios

of V2X communication and its performance requirements. LTE-V2X is a wireless communication technology for V2X with high data rate and controlled QoS [11,12], which is based on the evolution of LTE mobile communication technology defined by 3GPP, including two kinds of working modes of cellular communication (Uu) and direct communication (PC5) [13–16]. The Uu mode uses the existing LTE cellular network to implement V2V communication by forwarding (shown in Figure 1a), and the PC5 mode is similar to the DSRC, enabling direct communication between vehicles (shown in Figure 1b) [17,18]. 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.) [19].

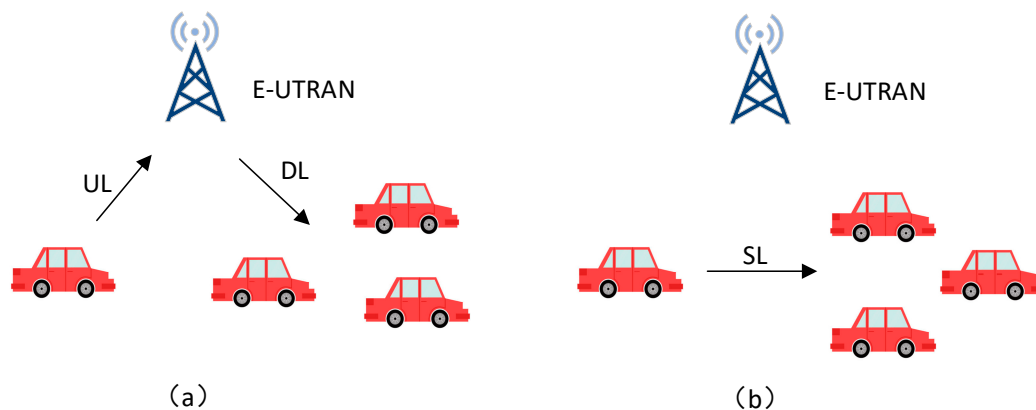


Figure 1. LTE-V2X Communication Modes. (a) Uu mode for LTE-V2X (b) PC5 mode for LTE-V2X.

The application of V2X involves many aspects, such as intelligent transportation, intelligent connected vehicles, and automated driving [20]. Different applications have different requirements for latency, reliability, throughput, user density, and safety of the V2X environment [21]. Safety applications and automated driving require extremely low latency and a secure network environment [22,23]. For example, vehicles usually spend most of their time moving at high speed and malicious attackers could cause serious traffic accidents by broadcasting false messages. Malicious attackers may also obtain a vehicle owner's identity information, vehicle location information, driving trajectory, and so on by interception of data packets [24]. This violates user privacy. The V2X data includes information about roads and geography, which relates to national security. Therefore, security is the top priority for V2X [25].

Testing is an important mean to ensure the safety and security of a vehicle. The V2X test is conducted to identify specification flaws, design flaws, and implementation defects over the entire life cycle, and to determine the root cause of the problem [26]. Modeling, analyzing, testing, and evaluating the security threats to V2X can help to improve the security protection capabilities of vehicles and promote the construction of vehicle security systems. In addition, by carrying out testing for V2X, we can pave the way for the commercialization of automatic driving and other applications.

The structure of this paper is as follows: Section 2 summarizes the types of V2X applications. Section 3 analyzes latency/reliability challenges and security challenges and summarizes the possible security threats. Section 4 describes why we need to do V2X tests and which types of tests should we do. Section 5 lists and briefly analyzes the test objectives and test methods of V2X. Section 6 proposes an end-to-end testing system combining virtual and real environments which can undertake the test task of the full protocol stack.

2. V2X Applications

The V2X represents a new cross-industry event involving automobiles, transportation, communications, and the Internet. Various industries and cross-industry alliances have researched the requirements for business applications of V2X. Currently, applications that have been developed or that

will be applied in the short term can be classified into three categories: safety applications, efficiency applications, and information services applications [27]. Safety applications refer to applications involving personal safety, such as collision warnings, road hazard warnings, and speeding warnings. Efficiency applications refer to applications that guide owners to drive and improve traffic efficiency, such as green wave speed guidance and congestion warnings. The information services applications refer to applications that provide owners with vehicle-related information to improve the driving experience, such as eCall, traffic information and route recommendations, and automatic parking. With the development of communication technology, the V2X will gradually meet the requirements for advanced automatic driving and applications in intelligent traffic systems. 3GPP defines four types of applications for these advanced application scenarios: Vehicle Platooning, Advanced Driving, Extended Sensors, and Remote Driving [22]. The above applications are all new applications resulting from the development of V2X. However, many traditional mobile applications will gradually enter the V2X industry, such as entertainment services.

3GPP has developed corresponding requirements for different V2X applications, among which latency/ reliability requirements and safety requirements are the top priorities [23]. The above applications are classified according to latency/reliability and security in Figure 2. The abscissa indicates the application's requirement for latency and reliability. The larger the abscissa is, the lower the latency required for the application, and the higher the reliability. The ordinate indicates the application's requirement for security, and the greater the ordinate is, the higher the security level of application security.

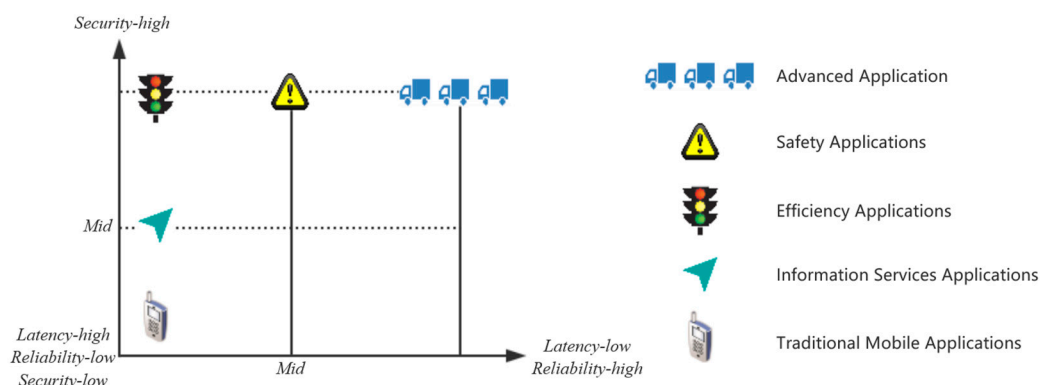


Figure 2. Vehicular Network Applications.

3. V2X Network Challenges

3.1. Latency/Reliability Challenges

The performance of the network is most important for applications which require low latency and high reliability. DSRC uses CSMA/CA to achieve collision avoidance and the ability for multi-user access. With fewer vehicles, DSRC has lower latency and higher reliability, but its performance is opposite in a dense vehicle environment. The latency of LTE-V2X is relatively stable, and the communication delay based on the PC5 interface, which can provide predictable delay and less interference is lower than 100 ms [28]. In the future, 5G networks will provide a communication delay of less than 1 ms while providing a stability of 99.999%, so they will be able support automatic-driving-oriented V2X services.

The V2X network faces many kinds of attacks which could lead to reduced performance. Denial of service (DoS) or distributed DoS (DDoS) refer to intensive use denial attacks by internal or external attackers on target nodes, resulting in the exhaustion of network resources and service resources [29]. They can cause serious problems, such as high latency of communication networks, network unavailability, and unavailability of node services. Jamming attacks and greedy behavior attacks, are examples of DoS attacks [30]. A jamming attack is an attack on the physical layer. The attacker jams the wireless channel through electromagnetic interference, which increases the

latency of the V2X communication and reduces the network's reliability [31]. A greedy behavior attack refers to a network node that violates the rules of channel access and occupies too many channel resources, thereby reducing the performance of other nodes and causing network congestion [32].

3.2. V2X Security Threats

The network security is an important part of V2X technology and the threats faced by V2X are divided into four aspects: mobile terminal security threats, V2X service platform security threats, V2X communication security threats, vehicle network data and privacy threats [33].

The combination of mobile smart terminals such as mobile phones and V2X can not only provide information and entertainment services for car owners, but also provides the function of remotely controlling vehicles. Mobile smart terminals typically connect to wireless networks such as in-vehicle Wi-Fi networks or Bluetooth, which provides malicious attackers with a springboard to the in-vehicle network. Moreover, applications on the mobile terminal are vulnerable to hackers because of its low threshold of development and easy accessibility.

The cloud service platform not only faces the problems of traditional network cloud platforms, but also has a weak identity authentication problem caused by the principle of mutual trust in V2X communications [33]. Whether the data in the cloud will be leaked is a major problem [34]. Moreover, the V2X cloud platform contains data about vehicles, roads, and pedestrians. If these data are leaked, they could cause significant losses. Owing to the high-speed mobility of vehicles, identity authentication and establishing a trusted connection with the cloud is a difficult problem. How to identify false data uploaded by an attacker and how to uniformly manage different types of data uploaded by different vehicles are also challenges faced by the cloud platform [35].

Because of its wireless transmission properties, the V2X network is particularly vulnerable to attacks. Therefore, communication security is very important. The security attributes include authentication, availability, data integrity, confidentiality, non-repudiation, real-time constraints, and attacks against these security attributes are as follows [30,36–39]:

- Authentication: Sybil attack, GPS spoofing/position faking attack, Node impersonation attack, etc.
- Availability: DoS attack, DDoS attack, Jamming attack, black hole attack, etc.
- Data Integrity: Masquerading attack, Replay attack, etc.
- Confidentiality: Eavesdropping attack, Traffic analysis attack, etc.
- Non-repudiation: Loss of events traceability, etc.
- Real-time constraints: Timing attack, etc.

According to the attacker's network location, attackers can be divided into insiders and outsiders. Insiders can communicate directly with other vehicles, but outsiders cannot. According to the purpose of attackers, they can be divided into malicious attackers and rational attackers. Malicious attackers destroy the network, not considering personal interests, while rational attackers do so to achieve personal benefits. According to the attack mode, attackers can be divided into active attackers and passive attackers. Active attackers actively send packets, but passive attackers only monitor a network. According to the scope of activities, attackers can be divided into local attackers and extended attackers. Local attackers only act within a limited range of activities, while extended attackers expand their range of activities by controlling other nodes [36,40].

Compared with the traditional network, the data on the V2X network is more open, so it is easier to expose more privacy data. Attackers can passively intercept user data or actively invade vehicles or cloud service platforms to steal information. In addition, mobile terminals such as smart phones also have the risk of privacy exposure. User privacy data such as the owner's name, plate number, vehicle speed, and driving route should be prevented from being acquired by others. However, some user privacy data must be open to trusted third parties such as police and accident rescue to ensure timely handling of emergencies such as accidents while being able to detect and track malicious attackers [41]. At present, V2X is in the initial stage of development. The data management and

privacy protection systems are still in the process of being perfected. It is necessary to discuss and refine key issues such as which data can be collected, how data is used, and whether it can be shared with third parties [33].

4. The Need for V2X Testing

Since vehicles usually spend most of their time moving at high speed, it may have serious consequences when an accident happens and even threaten the safety of the driver and passengers [42]. Safety always has the highest priority, so how to ensure vehicle safety has always been a serious topic. In the field of traditional automobiles, various testing and evaluation systems have been established in all world countries. Testing is an indispensable part of the Internet of Vehicles which is a new thing for us. If a vehicle receives erroneous data in a specific environment such as a highway or a crowded area, it may cause false triggering of a safety application, resulting in a serious traffic accident. Testing can ensure the reliability of the communication, thus ensuring the safety of the entire V2X environment. Because of the high requirements for security of the V2X, the priority of V2X testing is also high.

There are many problems in the Internet of Vehicles, which seriously hinder the development of vehicle networking technology and commercialization. Firstly, in special scenarios such as intersections or traffic jams, the density of vehicles is very large. The sheer number of users puts tremendous pressure on wireless communications, so it easily causes communication congestion [43]. Secondly, the vehicle has the characteristics of high mobility and rapidly changing network topology [44], which brings great difficulties to data transmission, routing, etc [45]. For example, two vehicles traveling in opposite directions will drive out of communication range within a few seconds. These communications have the requirement of low latency and high reliability for the Internet of Vehicles [46]. Finally, how to design and develop a good application is also an important issue for the Internet of Vehicles [47]. Before developing an application, developers need to spend a lot of time trying to determine the application scenarios. In addition, how to ensure the safety and effectiveness of an application is also an important issue [48].

Internet of Vehicles is a new cross-industry thing involving many industries such as automotive, communications, transportation, etc. As the name implies, V2X needs to connect all vehicles together, so the interconnection and interoperability are important attributes [49]. In the Internet of Vehicles, if a vehicle cannot understand the data sent by another vehicle with different brand, it will cause the lack of the information, and greatly reduce the meaning of V2X. Besides it may also lead to serious accidents resulting in unnecessary loss. At present, countries in which the V2X is growing up have been developing communication standards to help vehicles and other transportation participants to communicate unimpeded. These standards can also achieve understanding between different brands of vehicles and different intelligent transportation infrastructures, to ensure interconnection and interoperability of the V2X.

Testing aims to ensure safe and effective use of the Internet of Vehicles. Different testing methods are adopted for different needs. Communication standards, as a common language among vehicles, infrastructures, clouds, etc., can help vehicles communicate with other traffic participants accessibly, enabling the interconnection and interoperability. Interoperability testing can ensure information exchange and coordination between devices [50]. The protocol conformance testing aims to verify the conformity of each manufacturer's terminals with standards [51]. They lay a foundation for the interconnection and interoperability between different manufacturers' devices. Different V2X applications have different communication performance requirements [52], such as automatic driving needing extremely low latency, and video entertainment applications requiring larger bandwidth. The performance testing is mainly used to test the performance of the V2X network in different scenarios, including latency, communication range, packet loss rate, etc., to ensure that communication can meet the needs of the applications. Ensuring the safety, effectiveness and reliability of V2X applications is also an important goal of testing. The function testing can determine whether an application is valid, whether it can be triggered correctly in a specific scenario, and whether it can ensure vehicles safety.

Malicious applications will be removed after function testing. In general, we need to test functionality, performance, interoperability and consistency of the V2X terminal.

5. V2X Testing Methods

At present, V2X technology is in the exploratory stage. The traffic safety problems and information security problems brought about by its application have not yet been verified, so testing is an important part of V2X. 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. After laboratory testing, V2X applications must undergo field testing before they can be used commercially. Field testing is mainly used to evaluate the performance of V2X applications in a real environment and to meet the performance and function requirements in a large-scale environment.

5.1. Conformance Testing

Protocol conformance is the basis of V2X communication. Only by meeting the protocol conformance can we ensure the interoperability between vehicles, pedestrians, RSU, cloud platform, and other participants, which is the basis for developing various types of V2X applications. The protocols can be divided into two major categories. One is the communication protocol, which stipulates the data format and interaction flow of the communication processes in a V2X network, and the other is the security protocol, which stipulates the security processes such as certificates and authentication. Communication protocol conformance testing can ensure the interconnection and interoperability of devices [53], and security protocol conformance testing ensures security. Therefore, protocol conformance testing is a must-have requirement for all telematics devices.

ETSI stipulates an abstract test system for V2X conformance testing [54]. There are many ways to implement this abstract test system. ETSI recommends using TTCN-3 [55] to implement the abstract test system, as shown in Figure 3. This implementation conforms to ISO 9646 [56].

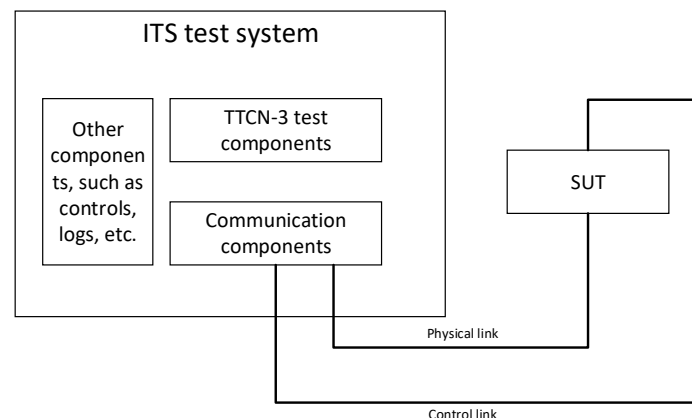


Figure 3. Abstract Test System [54].

3GPP provides a TTCN-3 based test system architecture [57], as shown in Figure 4, which is similar to the ETSI abstract test system. The difference is that the TTCN-3 test system (Host-PC in Figure 4) communicates with the device under test (UE in Figure 4) through the System Simulator hardware (HW). The test system is combined with the System Simulator HW, which is equivalent to a complete and controllable communication device that can fully test a device under test according to test cases by automatically or manually simulating communication processes.

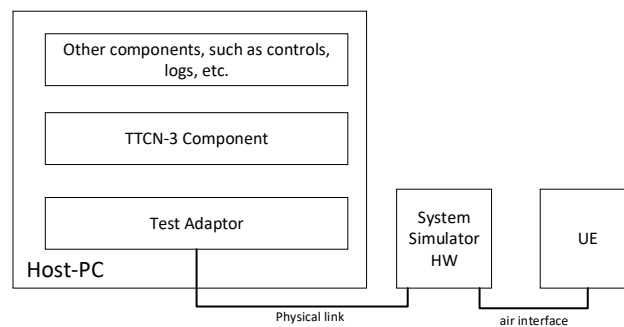


Figure 4. Test System Architecture Based on TTCN-3 [57].

In addition, ISO TS 20026 [58] also describes several similar ITS test architectures, which are generally indistinguishable from the above test architecture.

In order to support the conformance testing and enhance the completeness, test specifications have been proposed. For example, the Certification Operating Council (COC) under the U.S. Department of Transportation has established a series of specifications for conformance testing. In China, the C-V2X WG under IMT-2020(5G) promotion group also have established specifications for conformance testing, function testing and etc. Fouchal [59,60] designed a set of tools that could be used in order to check the conformance of a Cooperative-Intelligent Transport System (C-ITS). But there are still many challenges during the process of conformance testing. Firstly, due to the complexity of the standards, conformance testing needs to test every field in that standards which mean we need to design a large number of test cases. If a tester manually does a test, a lot of time will be wasted and there may be many mistakes during the testing process. So, the automated testing system has been developed. Its advantages are saving time and decreasing mistakes. But additional development needs to be done by the equipment developer because the automated testing system need control the device under test through a test control interface (TCI). The more complicated the test process is, the more additional development may be. So how to push the manufacturers to do the automated testing is a big question. Secondly, how many test cases are sufficient is another question. Test cases in conformance testing not only need to cover all the fields of the standards, but also need to test the understanding of the specific fields. For example, the representation and unit of longitude and latitude maybe differ. These confusions are mostly caused by the vague description in the standards and the conformance testing is a nice feedback to these standards. Finally, the above implements for conformance testing are all black-box, and they lack information or knowledge of system under test (SUT) [61]. Therefore we can't confirm whether a device under test transmits data by its protocol stacks. If the test cases have vulnerabilities, the manufacturers may develop a special program only for conformance testing instead of the part which is difficulty to develop in their device.

5.2. Function Testing

Application function testing can be used to determine whether an application can be triggered and take reasonable actions in different scenarios. It can guarantee the reliability and effectiveness of V2X applications. According to the environment, function testing can be divided into two types: laboratory testing and field testing. There is no doubt that the field testing is closest to reality. But if we want to do the V2X field testing, the testing scenarios will cost a lot of time and money. Besides, most of the scenarios are hard to build and the number of scenarios is huge. So a virtual function testing system in the lab is a perfect solution.

A virtual function testing system can be built only by software simulators, which means that all the testing scenarios are virtual. Aramrattana and Larsson [62] presented a simulation framework for testing and evaluation, which was aimed to test platooning. They used VTI for driving simulation and Plexe for traffic and network simulations. All the simulations were virtual and the framework had advantage that it was cheap to build and easy to extend its function such safety warning. But it depended

severely on the models such as communication model and traffic model. If a model didn't accurately reflect the real situation, the result of testing could be wrong leading invalid testing. Mittal and Savita [63] contrasted several simulators for VANETs which were old but some of them has been updated. They did the comparative study from the aspect of software characteristics, graphical user interface, accuracy of simulation, ease of use, popularity, input requirements and output visualization capabilities. Accuracy of simulation and ease of use were the most important for a simulator because they impacted directly on the testing results. Kim and Kim [64] had proposed a V2XREF of V2X Runtime Emulation Framework that can be used to perform the evaluation and validation of vehicle safety applications and safety systems along the various safety scenarios. Their emulation framework was also based software simulation and could be used in function testing. Schiller and Alois [65] had presented a new virtualization-based approach for emulating VANET by which application function testing could be performed. Choudhury [66] designed the simulation environment for V2X protocol and application testing. The test environment is divided into three parts, traffic simulators using VISSIM, network simulators using NS-3, and application simulators using MATLAB. The test environment adopts software simulation, so the underlying physical communication process cannot be tested. And because the tested application is not real and complete application software, it can only be tested against the application core algorithm and performance requirements. Ahmed [67] designed a test environment for testing V2X applications including three subsystems: input subsystem using NS-2, core subsystem to manage data and client framework subsystem providing a virtual test environment. Ming and Zhao [68] built a general testing framework based on Veins for securing VANET applications. Ribeiro and Gonçalves [69] tested a Platooning Management Protocol with VSimRTI framework.

The virtual simulation has its limitations which can't accurately reflect objective facts. Traditional Hardware-in-the-Loop (HIL) can be used in the V2X testing. Buse [70,71] proposed the Ego-Vehicle Interface (EVI) to integrate these very different types of simulators including HIL simulators and VANET simulators. Szendrei and Varga [72] designed a hardware-in-the-loop (HiL) V2X simulation framework to offer a cost-efficient and simple toolset. In the function testing with HIL, the device under test could be seen as a black-box and the testing environments were generated by the simulators. Its advantage is that we can test the V2X devices instead of the applications or algorithms. But it also faced the above problems because the testing environments were still virtual.

Our team is building a function testing system which extends the HIL methods. The system uses communication devices instead of the network simulator. The architecture is shown in Figure 5, including the V2X simulation platform, V2X communication module, GNSS simulator, channel interference unit, and CAN bus simulator. The V2X simulation platform performs application scenario simulation, test cases management, test result analysis, etc. It is used to generate dynamic simulation data of the vehicle, such as vehicle speed, position, distance between vehicles, obstacles, traffic scenes, etc., and manages the entire test activity. The V2X simulation platform generates a virtual traffic scenario based on the test cases. The scenario includes a host vehicle (HV) and at least one remote vehicle (RV). The host vehicle refers to the vehicle under test in this scenario, and the RV is used to assist the HV to trigger applications. The V2X simulation platform is connected to the V2X communication module through an Ethernet interface or similar to control the transceiver behavior of the V2X communication module. It also interconnects with the GNSS simulator and the CAN bus simulator through a serial or similar port, and sends the simulation data to the V2X communication module and the device under test. The V2X communication module is used to simulate a RV in a virtual traffic scenario to generate application messages such as a basic safety message (BSM), and then sends it to a device under test through the channel interference unit. Meanwhile, the V2X communication module can also receive application messages sent by the device under test. We have two methods to obtain the application messages of the V2X communication module. One involves the V2X simulation platform directly generating application messages and sending them to the V2X communication module, as shown in Figure 5a. The second involves the V2X communication module generating corresponding application messages according to the simulation data from the GNSS simulator and the CAN bus simulator,

as shown in Figure 5b. The channel interference unit simulates the communication environment, such as signal attenuation, interference, and so on. The device under test is used to simulate the HV in a virtual traffic scenario and runs V2X applications relying on simulation data. If the application is triggered, the device under test will generate a control action or warning information, which will be fed back to the V2X simulation platform through the CAN bus simulator. At this time, the HV will perform actions such as braking and issuing a warning, in the virtual traffic scenario.

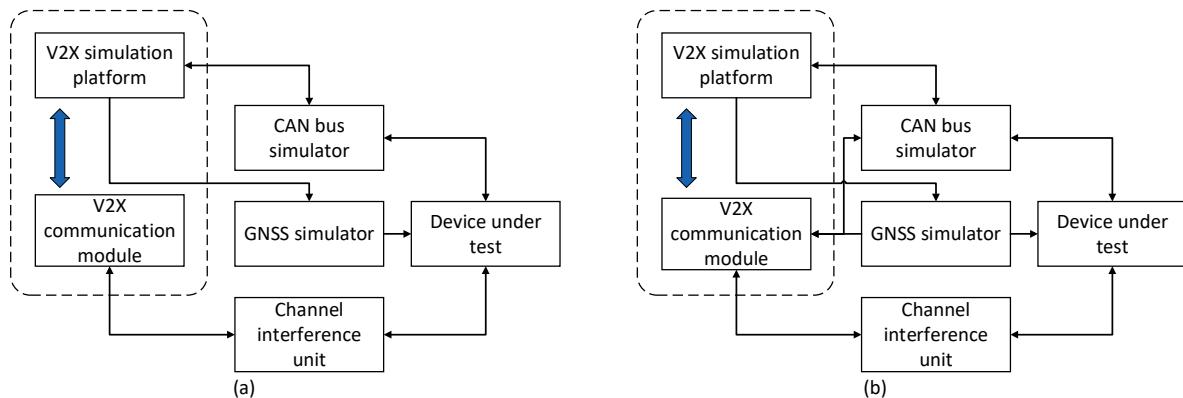


Figure 5. Function Test System Architecture. (a) the V2X simulation platform directly generates application messages and sends them to the V2X communication module; (b) the V2X communication module generates corresponding application messages according to the simulation data from the GNSS simulator and the CAN bus simulator.

There may be many problems in the function testing. Firstly, time synchronization is a big challenge for testing system. Because vehicles usually spend most of their time moving at high speed and the frequency of message transmission is very high, the unsynchronized vehicles will lead to trigger the applications wrongly. How to integrate real-time simulators and non-real-time ones guaranteeing time synchronization should also be considered before building the function testing system. Secondly, extra communication simulation delay that is the simulating delay minus the real delay such as V2V delay should be low. The extra delay may be generated due to the communication models. If the extra delay is high, the communication simulation can't reflect the reality. Finally, testing scenarios which is the key of function testing should cover special situations such as traffic jams, highway, mountain area and etc. In these extreme scenarios, application may perform bad.

5.3. Performance Testing

Performance testing is an important mean to guarantee the latency and reliability requirements of V2X applications. It mainly includes end-to-end communication delay testing, packet delivery success rate testing, and parameter testing, such as signal strength under different channels. Through performance testing, testers can understand the effects of basic network communications, and further determine whether the performance of network communications can support V2X applications.

Qin and Meng [73] implemented the 802.11p and 1609.3 protocols and tested the latency and packets loss in real filed. Carpenter and Sichertiu [74] developed a simulation to test the routing throughput, end-to-end delay and packet delivery ratio of a protocol in several VANET scenarios. Hiromori and Umedu [75] proposed a method for efficiently carrying out protocol testing for a set of designated node density distributions and their variations for VANET applications, network throughput, packet loss rates and etc. Vongpasith and Wang [76] analyzes routing protocol on the aspect of packet delivery ratio, average end-toend delay and throughput using a NS-2 simulator. Bouchra and Hicham [77] evaluated the packet delivery ratio, average end-to-end delay and bandwidth using a simulator based on NS2 and MOVE. Utkarsh and Raghavendra [78] testing the performance of the IEEE 802.11p standard for varying node density and data transfer rate by means of simulations

using NS-3. Huang and Zhao [79] studied the performance of DSRC based on Safety Pilot Model Deployment Data. Shi and Lu [80] evaluated the communication performance of Intersection Collision Warning(ICW) in field. Kawasaki and Onishi [81] investigated the performance of PC5-based and Uu-They are not the authors' surnames, please confirm.based LTE for crash warning application.

Now we have built a performance test-bed for black-box testing. The architecture of the test-bed is shown in Figure 6. The test system consists of three parts, including UEs (also referred to as user equipment, including the UE under test and the peer UE for simulating the process of transmission), the evolved core network (i.e., the MME/S-GW in Figure 6), and the evolved UMTS terrestrial radio access network (E-UTRAN). The channel simulator is used to simulate wireless channel propagation over the PC5 communication link. Network testers or other testing tools (such as test software developed by the device provider) are responsible for managing the testing process and receiving testing data. The UEs can connect with the E-UTRAN system through the TD-LTE air interface (i.e., the Uu interface). The system can test sidelink basic transmission under Mode4 and Mode3, and IOT test of RRC protocol performance. Based on the timestamps and packet numbers in the packet header, the transmission delays and packet delivery success rates of the packets are measured.

Most of the above works are mainly focused on the performance of a protocol using a simulator. However, equipment from different manufacturers may perform differently. So we need to test them using special testing methods and tools in the lab or filed. The lab testing could simulate a wide variety of performance testing environments, but it relies heavily on the model in simulators. The field testing is more realistic, but the extreme case is quite rare. Therefore, the performance testing meets the question of how to balance the lab testing with the field testing. The performance of V2X communication is also an important issue in the case of obstacles (such as buildings). To test performance in this scenario, modeling analysis and software simulation can be used [82–85]. In addition, lab testing can use channel simulators to generate non-line-of-sight communications. Testing performance in the case of obstacles does not require complex test scenarios, and only two communication terminals are required. Therefore, field testing is superior to lab testing.

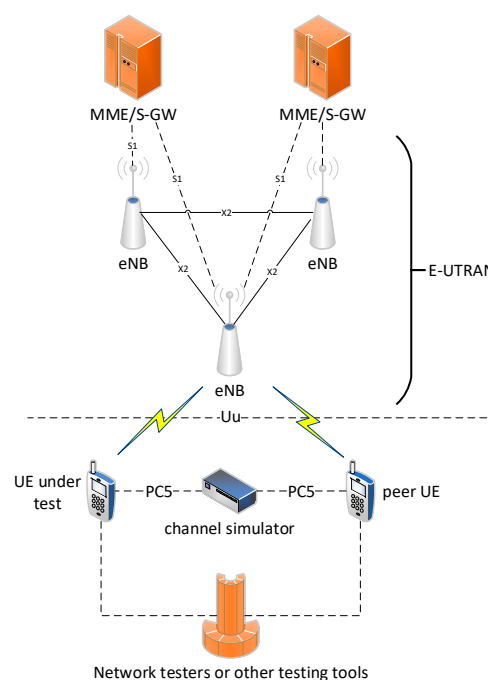


Figure 6. Terminal Performance Test System Architecture.

5.4. Vehicle Gateway Testing

Vehicle gateway testing is a mean to ensure that the vehicle gateway is running correctly, so it can meet the needs of V2X network security. The test architecture of the vehicle gateway is shown in Figure 7. The test architecture consists of two parts: the system under test and the test system. The system under test is composed of vehicle gateways and other systems or devices (including in-vehicle devices, networks, and service platforms), as shown by the dashed boxes in Figure 7. The test system is connected with the A-side and B-side of the system under test in Figure 7. 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 analyzing the differences of the expected results and the actual results obtained from the system under test. The test system supports inputting the test data and obtaining the results from the A-side and B-side in Figure 7 simultaneously.

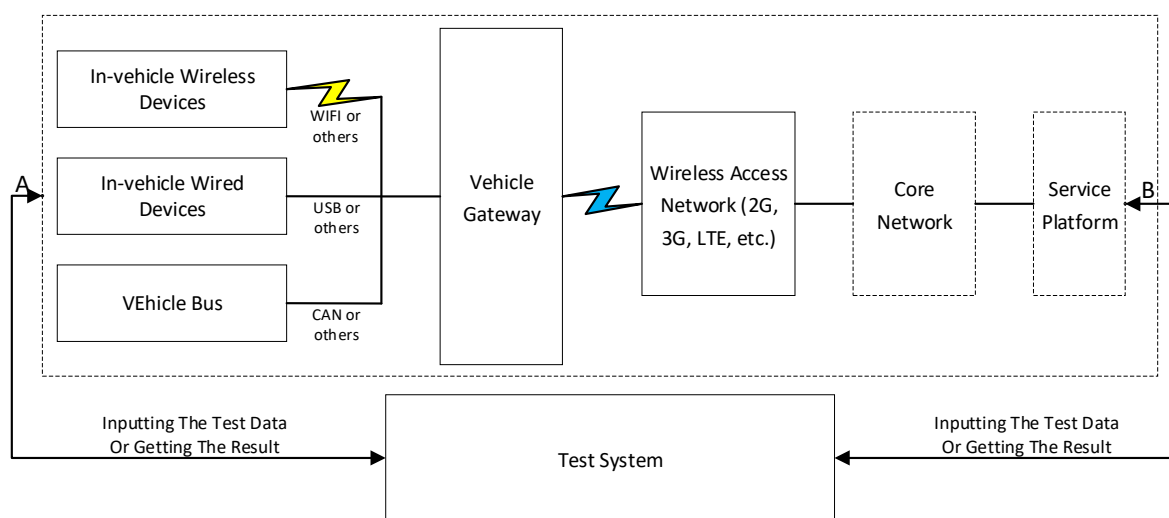


Figure 7. Vehicle Gateway Testing Architecture.

5.5. Penetration Testing

Penetration testing is a method of simulating a malicious attacker's methods and testing the security of the target system. It is a critical step in the development of the V2X. The penetration testing needs specific tools by which vulnerabilities of the V2X can be scanned [86]. The effectiveness of penetration testing relies on the skills and experience of testers [87], and it involves many disciplines, such as software, electronics, radio frequency (RF), and cryptography [26]. Therefore, penetration testing can be performed by personnel on an independent internal Cybersecurity test team or by outside third party engagement [88]. The penetration testing can be divided into three categories: white box testing, black box testing, and gray box testing [26,89]. In black box testing, the tests have no information regarding the tested system in advance, and they need to look for vulnerabilities from the perspective of the attacker. Its advantage is that the testing process is more realistic [90], but the disadvantage is also obvious—more testing time is needed. In white-box testing, testers can obtain information such as the design specifications of the system under test and code implementation in advance, making it easier to identify problems. However, the V2X is a complex system, and many design details should not be provided to testers, thus greatly reduces the advantages of white-box testing. Gray box testing is a mix of white box testing and black box testing which can obtain some information of the system under test and mainly adopts the white box test method. For the parts which testers cannot obtain information, the methods for black box testing are used. There are three types of specialized penetration testing: interface testing, transportation testing, and system testing [91]. Interface testing targets interfaces among the vehicles, mobile terminals, roadside units.

Transportation testing focuses on misuse issues and design flaws in communication protocols and weak cryptographic schemes. System testing examines the implementation flaws, insecure system settings and other known vulnerabilities of the vehicle gateways, vehicle systems, cloud systems, mobile terminal OSs, etc. And special penetration testing tools and techniques are needed to cover the above testing requirements.

The penetration testing process includes creating a threat model, designing a test plan, executing test cases, and generating test reports [92]. Creating a threat model can be based on the V2X security threats described in Section 3.2. Designing a test plan must guarantee availability of personnel or devices, meeting timelines and deliveries, comprehensive test cases, and adequate test tools. The process of executing test cases mainly focuses on system dependencies, user interfaces, system design, and system implementation. The test report is generated from the perspective of vulnerability reappearance, vulnerability severity assessment, and scenarios where malicious attackers exploit vulnerabilities.

Penetration testing generally adopts an iterative process. When a system vulnerability is discovered through testing, it is likely to expose additional problems. Therefore, testers can perform iterative testing based on the discovery of vulnerabilities. In addition, penetration testing can be combined with several other automated testing tools, using static analysis and dynamic analysis methods, reducing time and costs [93,94]. The test frameworks discussed in Sections 5.1–5.3 can also be used for penetration testing, for example, using test simulation devices for Sybil attacks, Replay attacks, etc., using channel jammers to simulate channel congestion scenarios. In addition to the test frameworks, those simulators mentioned above can be seen as the system under test. Then, testers can perform penetration testing to the simulators. 360, Visual Threat, Rapid7 and other companies have formed security teams to provide penetration testing services for communication protocols, mobile terminal APP, Cloud API, firewalls and etc.

5.6. Accelerated Testing

To solve the slow testing process of a vehicle, the accelerated test method can effectively reduce the cost and time spent on the vehicle reliability verification process [95]. Accelerated testing requires a significant amount of real-world data, and critical scenarios are used to analyze potential vehicle problems [96]. The analysis results will be applied to additional scenarios and the above process will be repeated. Some technologies such as importance sampling are used to accelerate the testing process [97]. Therefore, accelerated testing can greatly speed up a vehicle's test process. Accelerated testing can be used in lab simulations, human-in-the-loop tests with driving simulators, hardware-in-the-loop tests, or field testing [98]. Accelerated testing can also be used to test the reliability of the V2X in working conditions such as heavy rain, fog, and other extreme weather, and the network communications performance during traffic jams.

Some challenges should be considered before taking accelerated testing. One is that it performs badly in the field because it's hard to build the real-world environment. The other is how to build the model with the real-world data and how to ensure that iterative data is valid. From the perspective of communication, accelerated testing can be used in function and performance testing in the lab. For example, testers build the application scenarios according to the real world and generate new scenarios with the accelerated method.

5.7. Field Testing

The V2X network and its applications must be subjected to field testing and large-scale demonstration running before being officially promoted and used, such as the US's Safety Pilot Model Deployment [99], Security Credential Management System (SCMS) for vehicle-to-everything (V2X) communications [100], HarborNet [101], M-City, Safe intelligent mobility (sim^{TD}) [102], Korea Intelligent Transportation Demonstration in Jeju Island, China's 5+2 Internet of Vehicle Pilot Zones, etc. Waymo, Google's subsidiary for automatic driving, has conducted more than four million km of road testing [103]. Tesla has used simulators to test over several million km in conjunction with actual roads. Chinese

Internet companies such as Tencent and Baidu have also used simulators and road-testing methods to conduct extensive testing in demonstration zones. Unlike the traditional mobile applications, the V2X applications are deployed in the vehicles. So the tests of them need to be done in the field which is a big cost for the developer. In general, field testing requires a large number of basic network facilities and transportation facilities, test vehicles, testers, etc. So how to effectively reduce the cost of testing is particularly important [104].

Parallel testing can effectively reduce the cost of large-scale testing [105]. It belongs to the closed-loop hardware in the loop (HIL) test, which is mainly aimed to test the communication process and applications in the vehicle network and can provide a test environment for automatic driving. As shown in Figure 8, parallel testing can build a virtual test field based on an actual test field or create a complete virtual test field. The virtual test field includes a large number of virtual vehicles and virtual host vehicles. The host vehicles establish mappings with actual test vehicles or simulation cockpits. Other virtual vehicles use augmented reality (AR), sensor deception, mapping simulator communication devices, etc., to communicate with the test vehicles or simulation cockpits. Through the mapping of this virtual test environment to the real test environment, a large-scale test for V2X is realized.

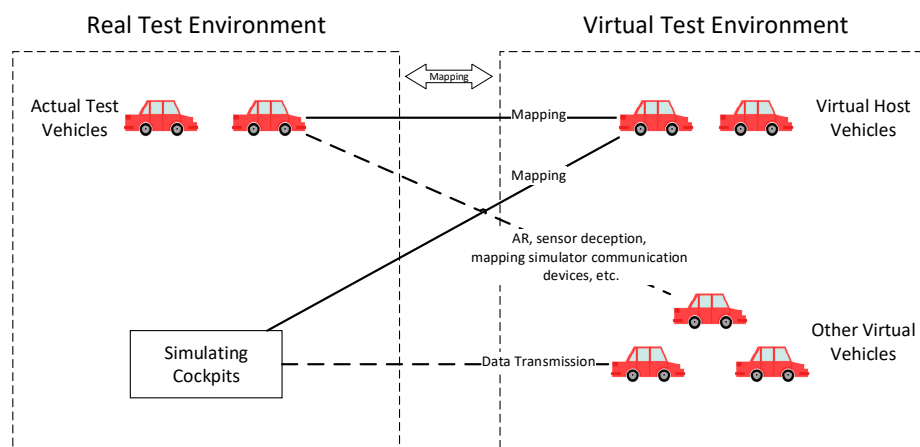


Figure 8. Parallel Testing Architecture.

5.8. Testing Tools

Testing tools are the basis of V2X testing. Many companies, organizations and research institutes have designed and developed a variety of testing tools. Spirent developed the 802.11p-based V2X Emulator to test V2X functionality and performance, and to support conformance testing of the WAVE protocol stack. OmniAir in the U.S. have developed DSRC conformance testing specifications and have conducted testing and certification work. In Europe, the 5GAA organizes cross-industry companies to establish a C-V2X test and evaluation system and has conducted corresponding large-scale field testing. Neusoft, Jilin University, etc. have developed cooperative perception sensing components and tools for testing in accordance with national standards. The V2X simulation runtime infrastructure (VSimRTI) was designed for the assessment of new solutions for Cooperative Intelligent Transportation Systems [106].

Science & Engineering Applications Datentechnik GmbH (S.E.A.) provides a complete V2X testing tool chain, including a series of V2X communication products and test systems, and provides customizing, support, and consulting services. Figure 9 shows the S.E.A. test tool set. The testing scope includes the application layer, network layer, access layer, and physical layer. The test architecture is similar to that discussed in Sections 5.1–5.3, but it is divided into two parts: open-loop test and closed-loop test. The open-loop test uses pre-designed scenarios to test the intrinsic behavior of the device under test. The closed-loop test adopts interactive driving scenarios to test platooning, dynamic controlling, and other interactive activities. NI also provides V2X test services, including PXI systems

for testing RF, m3 systems for testing GNSS, HIL test systems, and wireless test systems. For the applications and traffic scenarios, simulators are the main technology. Whether a simulator is excellent depends on the accuracy between its simulating output and the real world. For the communication, simulators are used to test the protocol. But in the actual testing process, communication devices usually be black-box and the channel may be simulated by testing tools. As for field testing, the communication environment is hard to build, because it is very expensive to build an extreme scenario such as traffic jam. Test tools mainly collect data in the field testing by which testers analyze the performance and function of a real vehicle application or device.

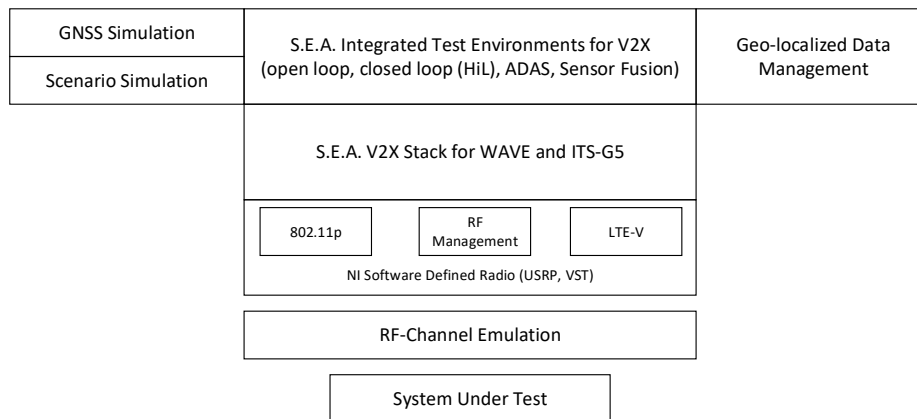


Figure 9. S.E.A. Testing Tools.

6. End-to-End Testing System Combining Virtual and Real Environments

From Section 5 we can see that current testing methods are independent and each of them have only one or two testing purposes, so we have proposed an end-to-end testing system combining virtual and real environments which can undertake the test task of the full protocol stack. The testing objects can be application function, protocol conformance, communication performance and etc. The system can be divided into three parts: scenarios, communication and applications.

The scenarios are the basis of the system and can be virtual, real or mixed. The virtual scenarios are used in the simulators to build the virtual testing environment. The real scenarios mean that the tests will be done in a field. We can use the real-world data to build the scenarios or map virtual objects to real scenarios which we call the mixed scenarios. One or more testing objects will be put into those scenarios. The communication connects all entities in the scenarios. The communication between virtual entities can be simulated by tools such as NS-3. But the communication between a virtual entity and a real entity is hard to handle. We can map the virtual entity to another real entity to transmit data in the real world or map the real entity into the virtual scenery to communicate with a simulator. Thus the communication has only two types: the virtual or the real. We also divided the applications into two types: virtual or real. The virtual application is the algorithm driven by a simulator in the virtual scenarios which can increase the integrity of the scenarios. The real application is one driven in a real device which is usually used as the background object.

We can combine all types of scenarios, communication or applications to build a test environment. For example, if we want to do a performance test for application layer protocol with low cost, we can choose the virtual communication whose network layer, access layer and physical layer are simulated. And forward collision warning in an on-board unit seen as a black-box can be tested with mixed scenario, real communication and virtual background application shown in Figure 5 which is easy to use and the cost is low.

7. Conclusions

As new technology, V2X not only provide a more comfortable and safer traffic environment, but also are important for improving traffic efficiency, reducing pollution, and reducing accident rates. The main V2X communication technologies are DSRC and LTE-V2X. There are many V2X applications, and their application requirements mainly focus on latency/reliability and security. Latency/reliability is threatened by the network performance problems and multiple types of malicious attacks. Security faces mobile terminal security threats, V2X service platform security threats, V2X communication security threats, vehicle network data and privacy threats. Testing is an important part of V2X. First, we describe the abstract test system and then introduce test methods from three perspectives: function, performance, and conformance. We then focus on testing methods such as vehicle gateway testing, penetration testing, and accelerating testing, and analyze the requirements for field testing. Finally, we have proposed an end-to-end testing system combining virtual and real environments which can undertake the test task of the full protocol stack.

Author Contributions: Conceptualization, J.W. and Y.S.; investigation, Y.S.; resources, Y.G.; data curation, R.Y.; writing—original draft preparation, Y.S.; writing—review and editing, J.W.; project administration, J.W.

Funding: This work was supported by the National Nature Science Foundation [61572229, and 6171101066]; Jilin Provincial Science and Technology Development Foundation [20170204074GX, 20180201068GX]; Jilin Provincial International Cooperation Foundation [20180414015GH] and CERNET Innovation Project [NGII20170413].

Conflicts of Interest: The authors declare no conflict of interest.

References

1. 5G Americas. (March 2018). Cellular V2X Communications Towards 5G. Available online: <http://www.5gamericas.org/en/resources/white-papers/> (accessed on 12 June 2018).
2. IMT-2020. IMT-2020 (5G) Promotion Group. (2018 Jun.). C-V2X Security White Paper. Available online: <http://www.imt2020.org.cn/zh/documents/download/82> (accessed on 30 June 2018).
3. USDOT. U.S. Department of Transportation. How Connected Vehicles Work. Available online: https://www.its.dot.gov/factsheets/pdf/connected_vehicles_work.pdf (accessed on 24 February 2018).
4. 5G Americas. (October 2016). V2XCellularSolutions. [Online]. Available online: http://www.5gamericas.org/files/2914/7769/1296/5GA_V2X_Report_FINAL_for_upload.pdf (accessed on 12 June 2018).
5. Kenney, J.B. Dedicated short-range communications (DSRC) standards in the United States. *Proc. IEEE* **2011**, *99*, 1162–1182. [CrossRef]
6. IEEE. *IEEE Standard for Information Technology—Local and Metropolitan Area Networks—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments*; IEEE Std 802.11p-2010; IEEE: New York, NY, USA, 2010.
7. IEEE. *IEEE Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages*; IEEE Std 1609.2-2016; IEEE: New York, NY, USA, 2016.
8. IEEE. *IEEE Standard for Wireless Access in Vehicular Environments (WAVE)—Networking Services*; IEEE Std 1609.3-2016; IEEE: New York, NY, USA, 2016.
9. IEEE. *IEEE Standard for Wireless Access in Vehicular Environments (WAVE)—Multi-Channel Operation*; IEEE Std 1609.4-2016; IEEE: New York, NY, USA, 2016.
10. SAE. *Dedicated Short Range Communications (DSRC) Message Set Dictionary*; J2735; SAE: Warrendale, PA, USA, 2016.
11. Araniti, G.; Campolo, C.; Condoluci, M.; Iera, A.; Molinaro, A. LTE for vehicular networking: A survey. *IEEE Commun. Mag.* **2013**, *51*, 148–157. [CrossRef]
12. Toukabri, T.; Said, A.M.; Abd-Elrahman, E.; Afifi, H. Cellular Vehicular Networks (CVN): ProSe-based ITS in advanced 4G networks. In Proceedings of the 2014 IEEE 11th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), Philadelphia, PA, USA, 28–30 October 2014.
13. 3GPP. *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Proximity-Based Services (ProSe); Stage 2 (Release 15)*; 3GPP TS 23.303 V15.0.0; 3GPP: Valbonne, France, 2017.

14. 3GPP. 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2 (Release 15); 3GPP TS 36.300 V15.0.0; 3GPP: Valbonne, France, 2017.
15. 3GPP. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Architecture Enhancements for V2X Services (Release 14); 3GPP TS 23.285 V14.3.0; 3GPP: Valbonne, France, 2017.
16. Uhlemann, E. Initial steps toward a cellular vehicle-to-everything standard [connected vehicles]. *IEEE Veh. Technol. Mag.* **2017**, *12*, 14–19. [[CrossRef](#)]
17. Chen, S.; Hu, J.; Shi, Y.; Peng, Y.; Fang, J.; Zhao, R.; Zhao, L. Vehicle-to-everything (v2x) services supported by LTE-based systems and 5G. *IEEE Commun. Stand. Mag.* **2017**, *1*, 70–76. [[CrossRef](#)]
18. Molina-Masegosa, R.; Gozalvez, J. LTE-V for sidelink 5G V2X vehicular communications: A new 5G technology for short-range vehicle-to-everything communications. *IEEE Veh. Technol. Mag.* **2017**, *12*, 30–39. [[CrossRef](#)]
19. 5GAA. (December 2017). An Assessment of LTE-V2X (PC5) and 802.11p Direct Communications Technologies for Improved Road Safety in the EU. Available online: <http://5gaa.org/wp-content/uploads/2017/12/5GAA-Road-safety-FINAL2017-12-05.pdf> (accessed on 1 January 2019).
20. Rebbeck, T.; Steward, J.; Lacour, H.A.; Killeen, A.; McClure, D.; Dunoyer, A. Final Report for 5GAA Socio-Economic Benefits of Cellular V2X. 5GAA. Available online: 5gaa.org/wp-content/uploads/2017/12/Final-report-for-5GAA-on-cellular-V2X-socio-economic-benefits-051217_FINAL.pdf (accessed on 1 January 2019).
21. 3GPP. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on LTE Support for Vehicle to Everything (V2X) Services (Release 14); 3GPP TR 22.885 V14.0.0; 3GPP: Valbonne, France, 2015.
22. 3GPP. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Enhancement of 3GPP Support for V2X Scenarios; Stage 1 (Release 15); 3GPP TS 22.186 V15.1.0; 3GPP: Valbonne, France, 2017.
23. 3GPP. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Service Requirements for V2X Services; Stage 1 (Release 14); 3GPP TS 22.185 V14.3.0; 3GPP: Valbonne, France, 2017.
24. Dolev, S.; Krzywiecki, Ł.; Panwar, N.; Segal, M. Dynamic attribute based vehicle authentication. *Wirel. Netw.* **2017**, *23*, 1045–1062. [[CrossRef](#)]
25. Yang, Y.; Wei, Z.; Zhang, Y.; Lu, H.; Choo, K.K.R.; Cai, H. V2X security: A case study of anonymous authentication. *Pervasive Mob. Comput.* **2017**, *41*, 259–269. [[CrossRef](#)]
26. Wooderson, P.; Ward, D. *Cybersecurity Testing and Validation*; No. 2017-01-1655; SAE Technical Paper: Warrendale, PA, USA, 2017.
27. CSAE. Cooperative Intelligent Transportation System; Vehicular Communication; Application Layer Specification and Data Exchange Standard; T/CSAE 0053-2017; CSAE: Beijing, China, 2017.
28. Chen, S.; Hu, J.; Shi, Y.; Zhao, L. LTE-V: A TD-LTE-based V2X solution for future vehicular network. *IEEE Internet Things J.* **2016**, *3*, 997–1005. [[CrossRef](#)]
29. RoselinMary, S.; Maheshwari, M.; Thamaraiselvan, M. Early detection of DOS attacks in VANET using Attacked Packet Detection Algorithm (APDA). In Proceedings of the 2013 International Conference on Information Communication and Embedded Systems (ICICES), Chennai, India, 21–22 February 2013.
30. Mejri, M.N.; Ben-Othman, J.; Hamdi, M. Survey on VANET security challenges and possible cryptographic solutions. *Veh. Commun.* **2014**, *1*, 53–66. [[CrossRef](#)]
31. Gross, J.; Punyal, O.; Pereira, C.; Aguiar, A. Experimental characterization and modeling of RF jamming attacks on VANETs. *IEEE Trans. Veh. Technol.* **2015**, *64*, 524–540.
32. Al-Terri, D.; Otrok, H.; Barada, H.; Al-Qutayri, M.; Al Hammadi, Y. Cooperative based tit-for-tat strategies to retaliate against greedy behavior in VANETs. *Comput. Commun.* **2017**, *104*, 108–118. [[CrossRef](#)]
33. CAICT. (2017 September). Vehicular Network Security White Paper. Available online: http://www.caict.ac.cn/kxyj/qwfb/bps/201804/t20180426_158472.htm (accessed on 2 June 2018).
34. Ghorbel, A.; Ghorbel, M.; Jmaiel, M. Privacy in cloud computing environments: A survey and research challenges. *J. Supercomput.* **2017**, *73*, 2763–2800. [[CrossRef](#)]
35. Yan, G.; Wen, D.; Olariu, S.; Weigle, M.C. Security challenges in vehicular cloud computing. *IEEE Trans. Intell. Transp. Syst.* **2013**, *14*, 284–294. [[CrossRef](#)]

36. Al-Kahtani, M.S. Survey on security attacks in Vehicular Ad hoc Networks (VANETs). In Proceedings of the 2012 6th International Conference on Signal Processing and Communication Systems (ICSPCS), Gold Coast, Australia, 12–14 December 2012.
37. Engoulou, R.G.; Bellaïche, M.; Pierre, S.; Quintero, A. VANET security surveys. *Comput. Commun.* **2014**, *44*, 1–13. [\[CrossRef\]](#)
38. Isaac, J.T.; Zeadally, S.; Camara, J.S. Security attacks and solutions for vehicular ad hoc networks. *Iet Commun.* **2010**, *4*, 894–903. [\[CrossRef\]](#)
39. Muhammad, M.; Safdar, G.A. Survey on existing authentication issues for cellular-assisted V2X communication. *Veh. Commun.* **2018**, *12*, 50–65. [\[CrossRef\]](#)
40. Hasrouny, H.; Samhat, A.E.; Bassil, C.; Laouiti, A. VANet security challenges and solutions: A survey. *Veh. Commun.* **2017**, *7*, 7–20. [\[CrossRef\]](#)
41. Bayat, M.; Barmshoory, M.; Rahimi, M.; Aref, M.R. A secure authentication scheme for VANETs with batch verification. *Wirel. Netw.* **2015**, *21*, 1733–1743. [\[CrossRef\]](#)
42. Xu, Q.; Mak, T.; Ko, J.; Sengupta, R. Vehicle-to-vehicle safety messaging in DSRC. In Proceedings of the 1st ACM International Workshop on Vehicular ad Hoc Networks, Philadelphia, PA, USA, 1 October 2004; ACM: New York, NY, USA, 2004.
43. Li, W.; Ma, X.; Wu, J.; Trivedi, K.S.; Huang, X.L.; Liu, Q. Analytical model and performance evaluation of long-term evolution for vehicle safety services. *IEEE Trans. Veh. Technol.* **2017**, *66*, 1926–1939. [\[CrossRef\]](#)
44. Oluoch, J. VANETs: Security Challenges and Future Directions. *World Acad. Sci. Eng. Technol. Int. J. Comput. Electr. Autom. Control Inf. Eng.* **2016**, *10*, 1033–1037.
45. Alotaibi, M.M.; Hussein, M. High speed multi-hop data dissemination for heterogeneous transmission ranges in vanets. In Proceedings of the 2015 IEEE International Conference on Ubiquitous Wireless Broadband (ICUWB), Montreal, QC, Canada, 4–7 October 2015.
46. Bai, F.; Krishnan, H. Reliability analysis of DSRC wireless communication for vehicle safety applications. In Proceedings of the Intelligent Transportation Systems Conference (ITSC'06), Toronto, ON, Canada, 17–20 September 2006.
47. Urra, O.; Ilarri, S. MAVSIM: Testing VANET Applications Based on Mobile Agents. In *Cognitive Vehicular Networks*; CRC Press: Boca Raton, FL, USA, 2016; pp. 199–224.
48. Fangchun, Y.; Shangguang, W.; Jinglin, L.; Zhihan, L.; Qibo, S. An overview of internet of vehicles. *China Commun.* **2014**, *11*, 1–15.
49. Gravina, R.; Palau, C.E.; Manso, M.; Liotta, A.; Fortino, G. *Integration, Interconnection, and Interoperability of IoT Systems*; Springer International Publishing: New York, NY, USA, 2018.
50. Eriksson, J.; Österlind, F.; Finne, N.; Tsiftes, N.; Dunkels, A.; Voigt, T.; Sauter, R.; Marrón, P.J. COOJA/MSPSim: Interoperability testing for wireless sensor networks. In Proceedings of the 2nd International Conference on Simulation Tools and Techniques, Rome, Italy, 28–31 July 2012; ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering): Brussels, Belgium, 2012.
51. Aho, A.V.; Dahbura, A.T.; Lee, D.; Uyar, M.U. An optimization technique for protocol conformance test generation based on UIO sequences and rural Chinese postman tours. *IEEE Trans. Commun.* **1991**, *39*, 1604–1615. [\[CrossRef\]](#)
52. 3GPP. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on Enhancement of 3GPP Support for 5G V2X Services (Release 15); 3GPP TR 22.886 V15.1.0; 3GPP: Valbonne, France, 2017.
53. Fouchal, H.; Wilhelm, G.; Bourdy, E.; Ayaida, M. A testing framework for intelligent transport systems. In Proceedings of the 2016 IEEE Symposium on Computers and Communication (ISCC), Messina, Italy, 27–30 June 2016.
54. ETSI. *Intelligent Transport Systems (ITS); Testing; Framework for Conformance and Interoperability Testing*; ETSI EG 202 798 V1.1.1; ETSI: Sophia Antipolis, France, 2011.
55. ETSI. *Methods for Testing and Specification (MTS); The Testing and Test Control Notation Version 3*; ETSI ES 201 873 (All Parts); ETSI: Sophia Antipolis, France, 2018.
56. ISO. *Information technology—Open Systems Interconnection—Conformance Testing Methodology and Framework*; ISO/IEC 9646 (All Parts); ISO: Geneva, Switzerland, 1994.

57. 3GPP. 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Packet Core (EPC); User Equipment (UE) Conformance Specification; Part 3: Test Suites (Release 14); 3GPP TS 36.523-3 V14.2.0; 3GPP: Valbonne, France, 2017.
58. ISO. *Intelligent Transport Systems—Cooperative ITS—Test Architecture*; ISO/TS 20026; ISO: Geneva, Switzerland, 2017.
59. Fouchal, H.; Bourdy, E.; Wilhelm, G.; Ayaida, M. A framework for validation of cooperative intelligent transport systems. In Proceedings of the 2016 IEEE Global Communications Conference (GLOBECOM), Washington, DC, USA, 4–8 December 2016.
60. Fouchal, H.; Bourdy, E.; Wilhelm, G.; Ayaida, M. A validation tool for cooperative intelligent transport systems. *J. Comput. Sci.* **2017**, *22*, 283–288. [[CrossRef](#)]
61. Lattarulo, R.; Heß, D.; Matute, J.A.; Perez, J. Towards conformant models of automated electric vehicles. In Proceedings of the 2018 IEEE International Conference on Vehicular Electronics and Safety (ICVES), Madrid, Spain, 12–14 September 2018.
62. Aramrattana, M.; Larsson, T.; Jansson, J.; Nåbo, A. A simulation framework for cooperative intelligent transport systems testing and evaluation. *Transp. Res. Part F Traff. Psychol. Behav.* **2017**. [[CrossRef](#)]
63. Mittal, N.M.; Savita, C. Comparative study of simulators for vehicular ad-hoc networks (vanets). *Int. J. Emerg. Technol. Adv. Eng.* **2014**, *4*, 528–537.
64. Kim, H.; Kim, T.; Kang, S.; Yoon, C.; Jung, J. Design of V2X runtime emulation framework for evaluation of vehicle safety applications. In Proceedings of the 2014 4th IEEE International Conference on Network Infrastructure and Digital Content (IC-NIDC), Beijing, China, 19–21 September 2014.
65. Schiller, M.; Alois, K. *Emulating Vehicular Ad Hoc Networks for Evaluation and Testing of Automotive Embedded Systems*; SimuTools: Athens, Greece, 2015.
66. Choudhury, A.; Maszczyk, T.; Dauwels, J.; Math, C.B.; Li, H. An integrated simulation environment for testing V2X protocols and applications. *Procedia Comput. Sci.* **2016**, *80*, 2042–2052. [[CrossRef](#)]
67. Ahmed, H.; Samuel, P.; Alejandro, Q. A flexible testbed architecture for VANET. *Veh. Commun.* **2017**, *9*, 115–126. [[CrossRef](#)]
68. Ming, L.; Zhao, G.; Huang, M.; Kuang, X.; Zhang, J.; Cao, H.; Xu, F. A General Testing Framework Based on Veins for Securing VANET Applications. In Proceedings of the 2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), Guangzhou, China, 8–12 October 2018.
69. Ribeiro, B.; Gonçalves, F.; Santos, A.; Nicolau, M.J.; Dias, B.; Macedo, J.; Costa, A. *Simulation and Testing of a Platooning Management Protocol Implementation*. *International Conference on Wired/Wireless Internet Communication*; Springer: Cham, Switzerland, 2017.
70. Buse, D.S.; Schettler, M.; Kothe, N.; Reinold, P.; Sommer, C.; Dressler, F. Bridging worlds: Integrating hardware-in-the-loop testing with large-scale VANET simulation. In Proceedings of the 2018 14th Annual Conference on Wireless On-demand Network Systems and Services (WONS), Isola, France, 6–8 February 2018.
71. Buse, D.S.; Christoph, S.; Falko, D. Demo abstract: Integrating a driving simulator with city-scale VANET simulation for the development of next generation ADAS systems. In Proceedings of the IEEE INFOCOM 2018-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Honolulu, HI, USA, 15–19 April 2018.
72. Szendrei, Z.; Varga, N.; Bokor, L. *A SUMO-Based Hardware-in-the-Loop V2X Simulation Framework for Testing and Rapid Prototyping of Cooperative Vehicular Applications*. *Vehicle and Automotive Engineering*; Springer: Cham, Switzerland, 2018.
73. Qin, Z.; Meng, Z.; Zhang, X.; Xiang, B.; Zhang, L. Performance evaluation of 802.11 p WAVE system on embedded board. In Proceedings of the 2014 International Conference on Information Networking (ICOIN), Phuket, Thailand, 10–12 February 2014.
74. Carpenter, S.E.; Sichiitiu, M.L.; Underwood, D.A.; Patwardhan, M.; Starr, S. Evaluating VANET Performance Using ns-3. WNS3 Workshop on NS-3. Available online: <https://www.semanticscholar.org/paper/Evaluating-VANET-Performance-Using-ns-3-Carpenter-Sichiitiu/7ffbacaef0a0842640f2f69b1b3a6746208c6e1> (accessed on 22 August 2018).

75. Hiromori, A.; Umedu, T.; Yamaguchi, H.; Higashino, T. Protocol testing and performance evaluation for manets with non-uniform node density distribution. In Proceedings of the IFIP International Conference on Testing Software and Systems, Aalborg, Denmark, 11–18 June 2012; Springer: Berlin/Heidelberg, Germany, 2012.
76. Phouthone, V.; Dong, W. Simulation based and analysis of routing protocols for vanet using vanetmobisim and NS-2. *Int. J. Comput. Eng. Technol.* **2015**, *6*, 32–41.
77. Marzak, B.; Toumi, H.; Benlahmar, E.; Talea, M. Performance analysis of routing protocols in vehicular ad hoc network. In *Advances in Ubiquitous Networking 2*; Springer: Singapore, 2017; pp. 31–42.
78. Prakash, U.; Pal, R.; Gupta, N. Performance evaluation of IEEE 802.11 p by varying data rate and node density in vehicular ad hoc network. In Proceedings of the 2015 IEEE Students Conference on Engineering and Systems (SCES), Allahabad, India, 6–8 November 2015.
79. Huang, X.; Zhao, D.; Peng, H. Empirical study of dsrc performance based on safety pilot model deployment data. *Parameters* **2017**, *12*, 14. [\[CrossRef\]](#)
80. Shi, M.; Lu, C.; Zhang, Y.; Yao, D. DSRC and LTE-V communication performance evaluation and improvement based on typical V2X application at intersection. In Proceedings of the Chinese Automation Congress (CAC), Jinan, China, 20–22 October 2017.
81. Kawasaki, R.; Onishi, H.; Murase, T. Performance evaluation on V2X communication with PC5-based and Uu-based LTE in crash warning application. In Proceedings of the 2017 IEEE 6th Global Conference on Consumer Electronics (GCCE), Nagoya, Japan, 24–27 October 2017.
82. Nguyen, H.; Liu, Z.; Jamaludin, D.; Guan, Y. A Semi-Empirical Performance Study of Two-Hop DSRC Message Relaying at Road Intersections. *Information* **2018**, *9*, 147. [\[CrossRef\]](#)
83. Zhang, X.; Miao, Q.; Li, Y. An Adaptive Link Quality-Based Safety Message Dissemination Scheme for Urban VANETs. *IEEE Commun. Lett.* **2018**, *22*, 2104–2107. [\[CrossRef\]](#)
84. Ali, G.M.N.; Rahim, M.N.A.; Chong, P.H.J.; Guan, Y.L. Analysis and improvement of reliability through coding for safety message broadcasting in urban vehicular networks. *IEEE Trans. Veh. Technol.* **2018**. [\[CrossRef\]](#)
85. Noor-A-Rahim, M.; Ali, G.M.N.; Nguyen, H.; Guan, Y.L. Performance Analysis of IEEE 802.11 p Safety Message Broadcast with and Without Relaying at Road Intersection. *IEEE Access* **2018**, *6*, 23786–23799. [\[CrossRef\]](#)
86. Bechtsoudis, A.; Nicolas, S. Aiming at higher network security through extensive penetration tests. *IEEE Lat. Am. Trans.* **2012**, *10*, 1752–1756. [\[CrossRef\]](#)
87. McDermott, J.P. Attack net penetration testing. In Proceedings of the 2000 Workshop on New Security Paradigms, Cloudcroft, NM, USA, 11–13 September 2001; ACM: New York, NY, USA, 2001.
88. SAE. *Cybersecurity Guidebook for Cyber-Physical Vehicle Systems*; J3061; SAE: Warrendale, PA, USA, 2016.
89. Whitaker, A.; Daniel, P.N. *Penetration Testing and Network Defense*; Cisco Press: Indianapolis, IN, USA, 2005.
90. McGraw, G. Software security. *IEEE Secur. Priv.* **2004**, *2*, 80–83. [\[CrossRef\]](#)
91. Chen, C.K.; Zhang, Z.K.; Lee, S.H.; Shieh, S. Penetration Testing in the IoT Age. *Computer* **2018**, *51*, 82–85. [\[CrossRef\]](#)
92. Thompson, H.H. Application penetration testing. *IEEE Secur. Priv.* **2005**, *3*, 66–69. [\[CrossRef\]](#)
93. Antunes, N.; Marco, V. Penetration testing for web services. *Computer* **2014**, *47*, 30–36. [\[CrossRef\]](#)
94. Arkin, B.; Stender, S.; McGraw, G. Software penetration testing. *IEEE Secur. Priv.* **2005**, *3*, 84–87. [\[CrossRef\]](#)
95. Zhao, D.; Huei, P. From the Lab to the Street: Solving the Challenge of Accelerating Automated Vehicle Testing. *arXiv*, 2017; arXiv:1707.04792.
96. Zhao, D.; Huang, X.; Peng, H.; Lam, H.; LeBlanc, D.J. Accelerated evaluation of automated vehicles in car-following maneuvers. *IEEE Trans. Intell. Transp. Syst.* **2018**, *19*, 733–744. [\[CrossRef\]](#)
97. Zhao, D.; Lam, H.; Peng, H.; Bao, S.; LeBlanc, D.J.; Nobukawa, K.; Pan, C.S. Accelerated Evaluation of Automated Vehicles Safety in Lane-Change Scenarios Based on Importance Sampling Techniques. *IEEE Trans. Intell. Transp. Syst.* **2017**, *18*, 595–607. [\[CrossRef\]](#)
98. Zhao, D. Accelerated Evaluation of Automated Vehicles. Ph.D. Thesis, University of Michigan, Ann Arbor, MI, USA, 2016.
99. Bezzina, D.; Sayer, J. *Safety Pilot Model Deployment: Test Conductor Team Report*; Report No. DOT HS 812. Available online: <https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/812171-safetypilotmodeldeploydeltestcondrtmrep.pdf> (accessed on 25 August 2018).

100. Brecht, B.; Therriault, D.; Weimerskirch, A.; Whyte, W.; Kumar, V.; Hehn, T.; Goudy, R. A Security Credential Management System for V2X Communications. *IEEE Trans. Intell. Transp. Syst.* **2018**, *99*, 1–22. [[CrossRef](#)]
101. Ameixieira, C.; Cardote, A.; Neves, F.; Meireles, R.; Sargento, S.; Coelho, L.; Afonso, J.; Areias, B.; Mota, E.; Costa, R.; et al. Harbornet: A real-world testbed for vehicular networks. *IEEE Commun. Mag.* **2014**, *52*, 108–114. [[CrossRef](#)]
102. Weiß, C. V2X communication in Europe—From research projects towards standardization and field testing of vehicle communication technology. *Comput. Netw.* **2011**, *55*, 3103–3119. [[CrossRef](#)]
103. Gomez, L.R.P.; Fairfield, N.; Szybalski, A.; Nemec, P.; Urmson, C. Transitioning a Mixed-Mode Vehicle to Autonomous Mode. U.S. Patent No. 8,078,349, 13 December 2011.
104. Xin, H.; Co, W.P. *Study on the V2X System Based on Vehicle Road Test*; Science & Technology Vision: Shanghai, China, 2016.
105. Wang, F.Y. Parallel control and management for intelligent transportation systems: Concepts, architectures, and applications. *IEEE Trans. Intell. Transp. Syst.* **2010**, *11*, 630–638. [[CrossRef](#)]
106. Schünemann, B. V2X simulation runtime infrastructure VSimRTI: An assessment tool to design smart traffic management systems. *Comput. Netw.* **2011**, *55*, 3189–3198. [[CrossRef](#)]



© 2019 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).

