DATA SECURITY CHALLENGES IN SELF-DRIVING CAR

Sara LAHDYA[1], Tomader MAZRI[2]

[1]University Ibn Tofail, National School of Applied Sciences Kenitra, Morocco – sara.lahdya@uit.ac.ma
[2]University Ibn Tofail, National School of Applied Sciences Kenitra, Morocco – tomader.mazri@uit.ac.ma

KEY WORDS: Autonomous vehicles, Security risks, V2X, 5G, 6G.

ABSTRACT:

As modern vehicles are sophisticated IoT devices with intelligence, capable of connecting to external infrastructure and utilizing vehicle-to-everything (V2X) communications, communications need to be secured so that cyberattacks do not reach their destination. In addition, the various organs of the car (sensors, communications, and controls) can have weaknesses that lead to accidents or potential fatalities. Automakers have a major responsibility for the safety of their customers and should not ignore important security research, but should ensure that important security measures are implemented that are less likely to attack your vehicle. This paper addresses the relevant attacks and threats to modern vehicles and presents a security analysis and possible countermeasures. We discussed the future of modern and autonomous vehicles and concluded that further countermeasures must be taken to create a future-proof concept.

1. INTRODUCTION

The future of internet-of-vehicle (IoV) and self-driving technology are booming. Then, these modern vehicles are loaded with technology, like sensors, entertainment systems, GPS, and autopilot (Lahdya & Mazri, 2021), that makes driving considerably safer and more dependable. The article discusses automation levels from level 4 to level 5. So, are these cars reliable to use? Could a malicious entity control the vehicles and put in danger? Finding the answers will require a very thorough study of the threats these cars will face in the future.

Automakers are attempting to stop security lapses and data hacks in new vehicles, but they are also introducing new and increasingly autonomous capabilities that could lead to new vulnerabilities and new threats. Cyberattacks are a very crucial threat to both industry and customers, security measures in these vehicles must keep up with new threats and new attack techniques that are developing as rapidly as the development of the Internet of Vehicles (IoV). (Abu Talib et al., 2018).

All the functions of the autonomous vehicle, they used to be mechanical or hydraulic, are now computerized; otherwise, the vehicle cannot be controlled by computer, (Says, 2022). Today, in building the software and hardware of modern self-driving cars, there are millions of lines of code behind. There are over 100 million lines of code that are placed in an autonomous vehicle, which must be checked for errors and bugs in order to be released safely to the public consumer.

In these last years, it seems that several groups of ethical hackers test these vehicles and their weaknesses in security, proving to the companies that the hardware or software design can be penetrated and violation of personal lives or collect location data for some people, (Tencent Keen Security Lab, 2019). They present an example of serious attack when the autopilot function was compromised in a Tesla Model S.

2. V2X AND FCD TECHNOLOGIES

V2X, FCD, and C-ITS technologies are used to enable communication between vehicles, infrastructures and, pedestrians, i.e. everything around the vehicle. In this part, we will start by studying the V2X technology and its various components. Next, we will explain the FCD technology.(Lecordier et al., 2018)

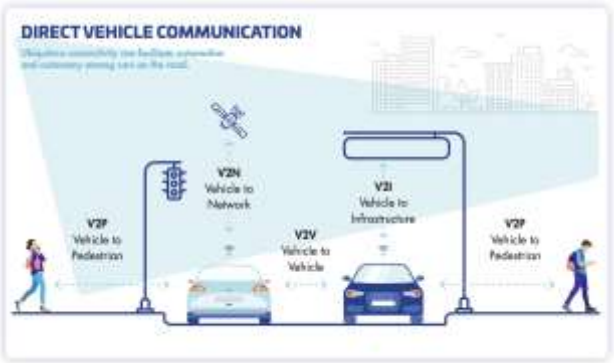

Figure 1. Direct vehicle communication

2.1 V2V technology

V2V, Vehicle-to-Vehicle. Began in 2006. It makes it possible to share the position of a vehicle as well as its movements with other equipped vehicles. This only works at short distances, but it is used to transmit the intentions of other drivers. It will therefore make it possible to streamline all road traffic, optimize it, and reduce traffic jams.(Garcia et al., 2021)

V2V technology uses multiple systems and networks to operate. On the one hand, it requires the use of antennas and sensors (Radars, Lidars, cameras...), 360˚ vision, but also the GNSS system that we will explain later. It also uses the intelligence of the vehicle. In the future, it seems obvious that 6G will not only take a very important place in V2X technology, but also in everything related to connected objects. V2V technology will nevertheless remain compatible with 2G, 3G, 4G, and 5G.(Campolo et al., 2017)

Figure 1. ©V2V communication Copyright 2017, 5GAA

2.2 V2I technology

In addition to V2V technology, V2I, Vehicle-to Infrastructure, It allows communication between vehicles and infrastructures, such as traffic lights or road signs. It also communicates signs for tunnels and bridges, such as speed limits, the dangers and prohibitions, as well as the maximum authorized weights and heights for vehicles. This technology itself uses another technology which is the FCD.

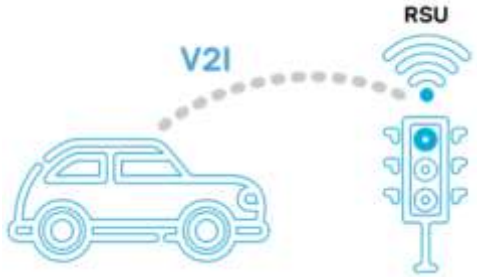

Figure 2. ©V2I communication Copyright 2017, 5GAA

2.3 V2P technology

V2P, Vehicle-to-Pedestrian, technology not only concerns pedestrian crossings and has the advantage of alerting drivers of autonomous vehicles, but also pedestrians of the potential dangers of accidents that exist, such as the fact that a pedestrian crossing crosswise and not straight, or intersections, where the pedestrian may be inconspicuous .(Zhou et al., 2020)

Figure 3. ©V2P communication Copyright 2017, 5GAA

In the event of almost immediate danger, an alert in the form of visual and audible signals is sent to the vehicle screen and to the pedestrian's telephone. In addition, the pedestrian's phone sends his activity to the vehicle: The driver can then know how the pedestrian is likely to be unaware, knowing if he is listening to music, sending a message, or calling someone.

This technology uses on the one hand the GPS system, but also the QZSS system and the DSRC.

2.4 V2N technology

The last V2X technology that we will present in this report is the V2N technology. It is a communication where one endpoint is a vehicle and the other endpoint is located in the Information and Communications Technology (ICT) infrastructure, is broadly defined as a set of physical components as well as software and network components.

Messages can be transmitted in both directions between endpoints. The vehicle uses cellular communications.(*5GAA-V2X-Terms-and-Definitions110917.Pdf*, n.d.)

Figure 4. ©V2N communication Copyright 2017, 5GAA

2.5 FCD technology

As mentioned above, FCD technology, Floating Car Data, is used, among other things, by V2I technology. This collects location and speed data, but also the direction of movement of vehicles.

All this data is collected using several networks. We can mention the GPS which communicates with the service provider, the cellular network GPRS, General Packet Radio Service, and the mobile phone of the driver which becomes a probe when it is switched on.

This data is ,therefore, used to know the traffic on the road networks, to calculate travel times and to generate precise reports on the state of the traffic by detecting traffic jams.

3. SYSTEMS

In this part, we will focus on four systems that allow autonomous vehicles to communicate. First, we will discuss about DSRC, GNSS, QZSS, and then we will explain C-V2X system. It is the latest communication technology in the IOV.

3.1 The DSRC

Dedicated Short Range Communication (DSRC) is a type of V2X technology that allows vehicles to communicate with other vehicles and infrastructure around them, by exchanging BSMs (Basic Safety Messages) in order to avoid all types of collisions. (Qualcomm Technologies, 2019)

DSRC is based on the IEEE 802.11p standard and has a data rate of less than 100Mb/s. (Abboud et al., 2016)

3.2 The GNSS

The GNSS system, Global Navigation Satellite System, is a satellite positioning system that was originally developed by the United States for military use. The advantages of this system are its worldwide coverage and its decametric precision which ensures the security of the system.

The system is based on a constellation of artificial satellites which, thanks to a receiver positioned in the vehicle, provide useful data to a user. These include the vehicle's 3D position, vehicle speed and time. Thanks to this data, the system can calculate the distance and the trajectory between these two satellites, i.e. the virtual satellite and the vehicle.

3.3 The QZSS

The QZSS system, Quasi-Zenith Satellite System, is a system under development by the Japanese space agency JAXA. The first trials of the system took place in 2010.

The system is based on the use of signals emitted by three satellites circulating in an orbit. It will allow positioning within a few centimetres.

3.4 The C-V2X

The C-V2X, Cellular-based Vehicle-to-Everything communication, is another vehicular communication system developed for V2X. Defined by the 3rd Generation Partnership Projects (3GPP), C-V2X uses cellular radio instead of WLAN, that means it uses the same set of cellular radio technology as cell phones. The C-V2X also defines two complementary transmission modes, namely: In direct C-V2X and Under Indirect C-V2X.

In direct C-V2X, vehicles communicate directly with other vehicles (V2V) and road units (V2I), via the PC5 interface Building on LTE direct device-to-device design with enhancements for high speeds / High Doppler, high density, improved synchronization and low latency.

Under Indirect C-V2X, vehicles communicate indirectly with other entities via the cellular network (V2N), through the Uu interface Using LTE to broadcast messages from a V2X server to vehicles and beyond. That DSRC cannot do. Vehicles can also send messages to the server via unicast.

Also, indirect C-V2X is useful because the cellular network can collect data from many cars and therefore can be more efficient in handling larger scale traffic. Originally designed in version 14 to use the LTE standard, 3GPP added later compatibility for 5G and 5G NR in versions 15 and 16.(AUTOCRYPT, 2021)

	DSRC	C-V2X	
Protocol Name	WAVE	3GPP Releases 14 3GPP later added 15, 16	
Communication	WLAN	Cellular (LTE,5G, 5G NR)	
		Direct C-V2X	Indirect C-V2X
Time of Deployment	2015	2021	2024
Cellular network connectivity	No	No	Yes

Table 1. The difference between DSRC and C-V2X systems

However, there are some similarities between DSRC and C-V2X: Both of them use the same message sets (SAE J2735 and J2945).(IWave Systems, 2020) . Also, they use digital signatures to ensure security and trust in message providers.

4. NETWORKS AND STANDARDS

In this part, we will focus on the different standards that allow autonomous vehicles to communicate. We will see which networks are already in place and which will replace.

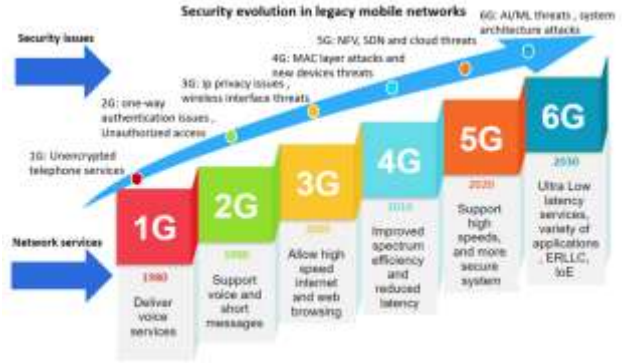

Figure 5. © The security evolution of mobile communications from 1G to the predicted future 6G Copyright 2022, Sensors

4.1 The 4G or LTE-Advanced standard

4G is a standard corresponding to the LTE-Advanced (Long Term Evolution) standard. This is a standard defined by the 3GPP standards body. The first version was completed in 2011, giving way to the 4G that we know. LTE-Advanced provides speeds greater than 1 Gb/s when stationary and greater than 100 Mb/s when the vehicle is in motion, even at over 120 km/h, unlike WiMax.

4.2 The 5G standard

5G had its first tests in 2018, with deployment planned for 2020. It is 100x faster than 4G and will therefore provide speeds ranging from 1 Gb/s to 10 Gb/s. This drastic increase in speed will make it possible to compensate for the proliferation of connected vehicles. This standard is based on millimetre waves, which cover high frequencies up to 300 GHz but which have the disadvantage of being unstable and at short range. In addition, we do not yet know the effects of these waves on health. (Lecordier et al., 2018)

In addition to the development of autonomous vehicles, 5G will make it possible to spread data mining, cloud computing and the interoperability of communicating objects. It will then allow connected devices to communicate with each other.

Regarding the security of this standard, we now know the solutions used to counter the possible failures of 5G. The first is the use of Small Cells: this is a large 5G antenna far from urban centres that distribute a signal to several smaller antennas located in the city centre. Small Cells therefore avoid overloading. The second solution provided is the use of MIMO, Multiple-Input Multiple-Output: This involves using hundreds of small antennas to multiply inputs and outputs. Thereby strengthening the signal and reducing interference.(Garakani et al., 2018)

4.3 The 6G standard

6G According to Samsung's projections, the 6G standard could be implemented from 2028, and could offer speeds 50 times greater than 5G, in the order of 125 GB/s with a latency of 0.1 ms. Soon, the world will experience independent, reliable, safe and cost-effective driverless vehicles that will spawn a new ecosystem of services. Which is created by introducing Autonomous Vehicle (AV) technology, such as, driverless taxis and driverless public transport... etc.

The most complex issues in Autonomous Vehicle security can be categorized into three areas, vehicle, supply chain and data collection. First, vehicle-level attacks can occur via the capture of car sensors, physical controls, and especially V2X (vehicle-to-everything) communications. In addition, using 6G networks, they can also assess situations and transmit messages triggered by the vehicle, as well as they can integrate security measures into a vehicle. Additionally, new types of V2X cyberattacks are possible in the AV ecosystem. Advanced AVs are connected to car manufacturers to continuously monitor software updates and send them to minimize predicted air issues.(Abdel Hakeem et al., 2022)

However, communication channel flaws, or the falsifying of data collected from the providers of cloud services, could have an impact on the security and safety of automobiles and their occupants. As a result, it is not easy to enable a uniform standard of safety standards and interoperability.(Abdel Hakeem et al., 2022)

Finally, AVs collect information about sensor data, travel routes, their passengers and builders, this can arise a problem of privacy and penetration by malicious entities. Therefore, the National Institute of Standards and Technology (NIST) Framework of Security in Autonomous vehicles, should ensure device security, data privacy, and security according to the National Institute of Standards and Technology. Protecting the personal privacy of 6G services is especially important when using public transportation modes such as planes, trains, and buses. Therefore, the security frameworks for autonomous vehicles must take into account security convergence by combining physical and digital safety as well as the idea of confidentiality by design. (Abdel Hakeem et al., 2022)

5. POTENTIAL SECURITY RISKS IN VEHICLES

5G is critical for future innovations in the fields of entertainment and infotainment, automated driving, and road safety. Several announcements ahead of MWC have been made by brands like BMW and Audi with major operator deals. Car manufacturers are moving forward to develop direct CV2X communication, which allows data exchange between vehicles and everything around them. It supports unified connectivity between entities connected in a V2X environment, vehicles, roadside equipment and mobile devices, allowing them to transmit information such as their current speed, position, direction, etc. and make smart decisions.(Says, 2022)

There are technological challenges with V2X, such as the interface of the V2X system, which requires an antenna module to connect the vehicle to all other networks reliably. Designing a V2X antenna is a challenge due to the complex environment in the vehicle, the tendency for hidden antenna solutions, the long simulation time, and the need for omnidirectional coverage. The adoption of 5G technology will be a game changer in the field, especially with the much faster internet connection speeds that come with it. This will also allow for faster and more efficient vehicle software updates. (VanYe et al., 2021)

Another challenge is that automakers are attempting to prevent security breaches and data hacks in new vehicles while also adding new, increasingly autonomous features that can expose new vulnerabilities. These two goals are often opposed. Nothing is ever completely secure in any complex system, as with security in any complex system. Even mastering this problem on multiple levels is difficult. Vehicle architectures today, and those being developed for future vehicles, are becoming increasingly complex, and are frequently beyond the control of a single company. As a result, there is still a long way to go before reaching the V2X environment.

Figure 6. © Vehicle security vulnerabilities possible Copyright 2022, Rambus

5.1 What does 5G mean for future customers:

• **Passengers** will be able to download or stream entertainment at faster and higher quality rates than ever before.

• **Vehicles** will be able to receive firmware and software updates over the air such as smartphones to help keep in-vehicle technology current and performing. (Kelarestaghi et al., 2021)

• **Infotainment and navigation systems** will be enhanced with HD/3D mapping and video, cloud-based user profiles, and mobile retail capabilities. (Kelarestaghi et al., 2021)

• **C-V2X (Cellular vehicle-to-everything) technology**, that some manufacturer of autonomous vehicle are developing for customers, is designed to enable vehicles to respond to other vehicles and the infrastructure around them with low-latency alerts and messages. This technology will be critical for the development of automated vehicles and safety advances, such as providing a more complete view of vehicle environments beyond what drivers, vehicle cameras, GPS, and radar systems can observe.(Says, 2022)

5.2 Cyber threats and challenges in AV

As we know, AV uses V2X communications to collect and transfer information. As well as V2X communications are one of the most important components of intelligent transport systems. However, to achieve the full potential of V2X communications, many issues and challenges will be open and need to be resolved. In this section, we aim to elaborate on several challenges and future research, for secure, reliable and robust V2X communications.

5.2.1 Privacy preservation: vehicular communications will be the largest viable network in the future. the lives of thousands of human beings will depend on the information exchanged between the vehicles themselves, the infrastructures, and the networks. Because of the importance of the information exchanged and the enormous number of users, the environment of the vehicular networks will be more than hostile. Indeed, messages related to road safety can be falsified or eliminated by malicious entities in order to cause accidents and endanger people's lives. Therefore, the major problem in vehicular networks is confidentiality. There are two things to think about before deploying these networks: identity privacy and location privacy.

To protect location privacy from malicious entities, there are additional policies that must be applied in addition to authentication. Until now, most methods proposed for location-based service (LBS) have involved eliminating location-related information to be sent to minimize security and privacy risks.
Therefore, a location preservation protocol which considered as the future research direction to protect the privacy of the location of LBS applications, while considering the aspects of power saving and storage capacity.(Huang et al., 2020)

5.2.2 Compatibility towards the heterogeneous networks: In the future, 6G-V2X will be the major radio access technology for V2X services, so new security solutions must take into account heterogeneity of 6G and 5G environment. Furthermore, the V2X services belong to the big family of Internet of Things, in which the heterogeneity of the network must be considered.

Furthermore, 6G-V2X brings not only challenges but also benefits, such as ultra-low latency and high data transmission rate. As a result, new solutions may be free of DSRC constraints and take advantage of the new network architecture.(Alalewi et al., 2021)

5.2.3 Security in Autonomous Vehicles : Autonomous vehicles have become more and more popular in recent years, and safety remains the most important requirement. They are an integration of many technologies and sensors like GPS, light detection and ranging (LiDAR), cameras, operating systems, cloud platforms, etc. (Alalewi et al., 2021)

However, to secure such an advanced autonomous vehicle system, various aspects must be taken into consideration. First, securing V2X services, which has a crucial role. Then three other aspects deserve attention, such as sensors, operating systems, and control systems. Sensors mounted on autonomous vehicles are responsible for collecting surrounding information, which can be the input of many algorithms. And they must be protected against jamming, identity theft and above all DoS attacks, which remains a huge challenge. When it comes to operating systems and control systems, the biggest issue is defining a correct authentication method to prevent attackers from hijacking the vehicle through any hardware port..(Alalewi et al., 2021)

DUSCUSSION

This communication forms a general discussion and thus gives us avenues for reflection and work to be carried out for the community of security practitioners and researchers. The autonomous vehicle is one of the most promising technological solutions capable of reducing road accidents, 90% accidents are due to human error. While the positive impact on accidentology of automatic action in a critical situation (loss of grip, emergency braking, etc.) has been widely demonstrated, it remains to be proven that an automated driving strategy is safer and more efficient than human driving in everyday use.
The task of autonomous driving is becoming extremely complex as a whole and must gradually be considered at the same degree of criticality as that applied in the aeronautical field. For example, in order to reduce technological risks. Each brick necessary for setting up a delegation of driving (navigation, perception, generation of trajectories and control) has its own level of complexity, linked both to the hardware part (sensors, actuators used) and to the software part (command and perception algorithms, etc.). The major difficulty is to understand the driving architecture of the autonomous vehicle as a whole. Indeed, the many interactions between these levels must be controlled because they are likely to generate side effects that are often difficult to predict during the design phases. Technological risks are diverse in nature (software and hardware) and are difficult to assess as a whole. Scientific and technical developments will therefore tend to initially make each level more reliable while ensuring that the whole remains coherent and safe.

Nowadays, we see that autonomous vehicles contain several systems and technologies to meet consumer`s expectations, but safety remains a major issue and challenge in AVs, especially as we are faced with a new technology that is 6G.

CONCLUSION AND FUTURE WORK

In the end, security remains a crucial issue that must be taken into consideration before the deployment of autonomous vehicles, and especially in V2X communication, which opens up several vulnerabilities to attackers. In this article, we have studied the different modes of communication of autonomous vehicles. Right after, we made a comparison between the DSRC systems and the C-V2X which is the most recent, without forgetting the 4G, 5G and 6G standards and their advantages in vehicular networks. Finally, we ended our article by citing the various cyber threats and challenges in autonomous vehicles. For our future work, we will work more on cyber threats and the various possible attacks on V2X communication. Thus, to propose more relevant solutions.

REFERENCES

5GAA-V2X-Terms-and-Definitions110917.pdf. (n.d.). Retrieved June 14, 2022, from https://5gaa.org/wp-content/uploads/2017/08/5GAA-V2X-Terms-and-Definitions110917.pdf

Abboud, K., Omar, H. A., & Zhuang, W. (2016). Interworking of DSRC and Cellular Network Technologies for V2X Communications: A Survey. IEEE Transactions on Vehicular Technology, 65(12), 9457–9470. https://doi.org/10.1109/TVT.2016.2591558

Abdel Hakeem, S. A., Hussein, H. H., & Kim, H. (2022). Security Requirements and Challenges of 6G Technologies and

Applications. Sensors, 22(5), 1969. https://doi.org/10.3390/s22051969

Abu Talib, M., Abbas, S., Nasir, Q., & Mowakeh, M. F. (2018). Systematic literature review on Internet-of-Vehicles communication security. International Journal of Distributed Sensor Networks, 14(12), 1550147718815054. https://doi.org/10.1177/1550147718815054

Alalewi, A., Dayoub, I., & Cherkaoui, S. (2021). On 5G-V2X Use Cases and Enabling Technologies: A Comprehensive Survey. IEEE Access, 9, 107710–107737. https://doi.org/10.1109/ACCESS.2021.3100472

AUTOCRYPT. (2021, January 19). DSRC vs. C-V2X: A Detailed Comparison of the 2 Types of V2X Technologies. AUTOCRYPT. https://autocrypt.io/dsrc-vs-c-v2x-a-detailed-comparison-of-the-2-types-of-v2x-technologies/

Campolo, C., Molinaro, A., Iera, A., & Menichella, F. (2017). 5G Network Slicing for Vehicle-to-Everything Services. IEEE Wireless Communications, 24(6), 38–45. https://doi.org/10.1109/MWC.2017.1600408

Garakani, H. G., Moshiri, B., & Safavi-Naeini, S. (2018). Cyber Security Challenges in Autonomous Vehicle: Their Impact on RF Sensor and Wireless Technologies. 2018 18th International Symposium on Antenna Technology and Applied Electromagnetics (ANTEM), 1–3. https://doi.org/10.1109/ANTEM.2018.8572847

Garcia, M. H. C., Molina-Galan, A., Boban, M., Gozalvez, J., Coll-Perales, B., Şahin, T., & Kousaridas, A. (2021). A Tutorial on 5G NR V2X Communications. IEEE Communications Surveys & Tutorials, 23(3), 1972–2026. https://doi.org/10.1109/COMST.2021.3057017

Huang, J., Fang, D., Qian, Y., & Hu, R. Q. (2020). Recent Advances and Challenges in Security and Privacy for V2X Communications. IEEE Open Journal of Vehicular Technology, 1, 244–266. https://doi.org/10.1109/OJVT.2020.2999885

IWave Systems. (2020). DSRC and C-V2X: Revolutionising Connected Mobility. iWave Systems. https://www.iwavesystems.com/news/dsrc-and-c-v2x-revolutionising-connected-mobility/

Kelarestaghi, K. B., Foruhandeh, M., Heaslip, K., & Gerdes, R. (2021). Intelligent Transportation System Security: Impact-Oriented Risk Assessment of in-Vehicle Networks. IEEE Intelligent Transportation Systems Magazine, 13(2), 91–104. https://doi.org/10.1109/MITS.2018.2889714

Lahdya, S., & Mazri, T. (2021). SECURITY STUDY OF ROUTING ATTACKS IN VEHICULAR AD-HOC NETWORKS (AUTONOMOUS CAR). The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences, XLVI-4/W5-2021, 349–353. https://doi.org/10.5194/isprs-archives-XLVI-4-W5-2021-349-2021

Lecordier, J., Marmin, F., Simoes Maricato, H., Lefebvre, C., Picard, L., & Zheng, T. (2018, June 17). Véhicule Autonome: Systèmescoopératifs/Communication. https://fr.readkong.com/page/vehicule-autonome-systemes-cooperatifs-communication-8359013

Qualcomm Technologies. (2019). Introduction to Cellular V2X. 23.

Says, S. P. (2022, February 3). Data Security Challenges In Automotive. Semiconductor Engineering. https://semiengineering.com/data-security-challenges-in-automotive/

Tencent Keen Security Lab. (2019, March 29). Tencent Keen Security Lab: Experimental Security Research of Tesla Autopilot. Keen Security Lab Blog. http://keenlab.tencent.com/2019/03/29/Tencent-Keen-Security-Lab-Experimental-Security-Research-of-Tesla-Autopilot/index.html

VanYe, C. M., Li, B. E., Koch, A. T., Luu, M. N., Adekunle, R. O., Moghadasi, N., Collier, Z. A., Polmateer, T. L., Barnes, D., Slutzky, D., Manasco, M. C., & Lambert, J. H. (2021). Trust and Security of Embedded Smart Devices in Advanced Logistics Systems. 2021 Systems and Information Engineering Design Symposium (SIEDS), 1–6. https://doi.org/10.1109/SIEDS52267.2021.9483779

Zhou, H., Xu, W., Chen, J., & Wang, W. (2020). Evolutionary V2X Technologies Toward the Internet of Vehicles: Challenges and Opportunities. Proceedings of the IEEE, 108(2), 308–323. https://doi.org/10.1109/JPROC.2019.2961937