SECURITY OF AUTONOMOUS VEHICLES: 5G IOV (INTERNET OF VEHICLES) ENVIRONMENT

Ouidad Saber, Tomader Mazri

National School of Applied Sciences, University Ibn Tofail, Kenitra, Morocco – (ouidad.saber, tomader.mazri) @uit.ac.ma

KEY WORDS: Autonomous Vehicles, 5G, Internet of Vehicles, Security attacks, Security solutions, Blockchain

ABSTRACT:

An autonomous vehicle is designed to move partially or totally without the intervention of the driver. It is a system equipped with sensors, communication and processing units that make it able to monitor and analyse traffic information in real time to improve road safety. In addition, Internet of Vehicles is the latest technology dedicated to autonomous vehicles, the integration of this technology with 5G serves as a platform to interconnect sensors, vehicles, infrastructure, pedestrian, and network. Hence, the 5G Internet of Vehicles environment provides significant benefits, including increased security, high reliability, wide communication coverage and low service latency. On the other hand, due to the ubiquity of network connectivity, it also presents serious confidentiality, integrity, and availability issues for autonomous vehicles. This paper provides an overview of the autonomous vehicle concept by highlighting its technologies and the 5G IoV environment, presenting some susceptible attacks that can touch the security of this environment, and some good practices to ensure the autonomous vehicle security.

1 INTRODUCTION

People are seriously injured or killed in traffic accidents due to human error, including driving errors (e.g., driver inattention and distraction, reckless driving and poor driving ability) and other road user errors (such as traffic violations). In addition, vehicle failures (e.g., brake failure) or environmental conditions (such as insufficient traffic information) can also affect road safety. Thus, to improve traffic efficiency, reduce traffic congestion, and promote sustainable transportation development, recent advances in information and communication technologies and the automotive industry have introduced a new type of vehicles, known as Autonomous Vehicles (AV).

A vehicle is considered fully autonomous when it is equipped with an automated driving system. It can circulate with passengers on any type of road, without any human intervention. An autonomous vehicle allows its passengers to be transported safely and it must be safe for other road users. The development of this type of vehicle requires administrations and car manufacturers to proceed in stages. They develop cars corresponding to different levels of autonomy, these levels are basically a progression of self-driving capability, ranging from 0 (no self-driving capability at all) to 5 (full self-driving capability) (Pham & Xiong, 2021).

Autonomous vehicles bring a new concept and model, which applies the new generation of information technologies, such as Internet of Things, cloud computing, wireless technologies, artificial intelligence, etc. In addition to these technologies, AV use numerous sensors (GPS, camera, radar, lidar, etc.) (Ahangar et al., 2021).

As an important branch of Internet of Things, the Internet of Vehicles (IoV) is used in urban traffic environment to provide network access for drivers, passengers and traffic management managers.

On the way to implement autonomous vehicles in our real life, there are many challenges that must be overcome. Thus, it is essential to provide efficient, reliable and in time communications to all vehicles and their embedded sensors, the demanding specifications such as high data rate, low latency, and high reliability in Internet of Vehicles make the fifth generation (5G) an emerging solution for addressing the current vehicular network challenges. Thanks to the emerging new technologies in the fifth generation, the IoV will support many types of communication especially Vehicle to Vehicle (V2V), Vehicle to Infrastructure (V2I), Vehicle to Cloud (V2N) and Vehicle to Pedestrian (V2P). (Garcia et al., 2021). However, the deployment of all these technologies and communication modes makes the 5G IoV environment open to different attacks such as Man-in-the- middle, Sybil, and Denial of Service (DoS) attacks (Lu et al., 2020).

The objective of this paper is to present an overview of the autonomous vehicles and the 5G IoV environment, the main cyberattacks concerning information and communication security, and some solutions to deal with these cyberattacks. The content of the paper is organized as follows: In Section 2 we present the autonomous vehicles and their vehicular network. Section 3, describes some 5G IoV environment attacks. Proposed solutions to address these attacks in Section 4. Section 5 is the results section that represents the convenient security solutions for each attack. Concluding by a discussion and conclusion in section 6 and 7.

2 AUTONOMOUS VEHICLES OVERVIEW

The Society of Automotive Engineers (SAE) classifies vehicles into six different levels of automation. Other organizations use the same classification, such as the International Organization of Automobile Manufacturers and the Federal Highway Institute (Ahangar et al., 2021). The detailed functional description of each level is as follows:

The first level is no automation where all the tasks are performed by the driver.

The second level is the driver assistance. This level refers to the models that are equipped with a cruise control or an anti-lock

This contribution has been peer-reviewed.
https://doi.org/10.5194/isprs-archives-XLVIII-4-W3-2022-157-2022 | © Author(s) 2022. CC BY 4.0 License.

system for example. Human presence is mandatory and the vehicle cannot do anything by itself.

The third level is the partial automation, which allows the vehicle to take control of speed, direction, and even the steering wheel in certain driving modes. Even with a car of this level of automation, the driver must remain at the steering wheel and monitor the environment.

The fourth level is the conditional automation. From this level, the vehicle is able to understand its driving environment and act accordingly. On the highway, for example, the car can overtake a vehicle on its own when the turn signal is activated. It is also capable of keeping the right safety distance and decelerating as soon as the driving situation requires it. Here again, the human is still indispensable when the autonomous car asks him to take control.

The fifth level is the high automation. This is only possible under certain conditions, such as on the highway. If something goes wrong, the car must be able to continue driving on its own without driver intervention.

The sixth level is the full automation. A level 5 autonomous car can drive on all types of roads, without the intervention of a driver. The driver can engage in other activities such as reading or watching a movie. The car drives him wherever he wants without him having to intervene. The car takes him wherever he wants without his intervention (Zanchin et al., 2017).

2.1 The functioning of autonomous vehicles

The functioning of autonomous vehicles is divided into four main steps described as follow:

Perception: This step consists of detecting the surroundings of the AV using various sensors and detecting its own position in the environment. The information from these sensors is then transmitted to the recognition modules which process this information.

Analysis: The information collected by all the sensors is routed to the car's brain (the computer software) which is based on artificial intelligence. It analyses, compares and gives meaning to data in real time.

Decision Making: Depending on the results of artificial intelligence analysis of the data, this phase decides, plans, and controls the AV's movements and behaviours. This stage is similar to the brain, making decisions such as path planning, action prediction, and obstacle avoidance.

Activation: The decision making step then leads to an action that activates or deactivates certain commands such as turning right, braking, accelerating, etc (Lakomicki, 2018).

After discussing how an autonomous vehicle work, we will discuss the design, function, and use of some of its main sensors.

Radar: It uses radio waves instead of light to detect the environment. There are two types of radars, millimeter radar and ultrasonic radar. Millimeter radar is used for object detection, and ultrasonic radar is used in short-range scenarios such as parking assist systems.

LiDAR: Laser Imaging Detection And Ranging is the most basic sensor in AV to support localization and parking assistance. It uses light point clouds to detect distances and boundaries of surrounding obstacles and the environment (Pham & Xiong, 2021).

Cameras: cameras are considered in autonomous vehicles as image sensors, they are placed in many locations to provide a 360-degree view around the vehicle. Cameras provide information for important autonomous tasks such as traffic sign recognition and lane recognition.
Cameras can also replace LiDAR for object detection and distance measurement at a lower cost, but perform poorly in certain situations such as rain, fog, or snow (Sun et al., 2022).

GPS: Global Positioning System is a global navigation system based on satellites in Earth orbit that emit high-frequency radio signals.
Radio signals can be picked up by many devices, such as smartphones and GPS receivers in autonomous vehicles. When GPS receivers detect signals from three or more satellites, they can calculate their positions (Bezai et al., 2021).

2.2 Vehicular networks

2.2.1 VANET

The main idea of vehicular networks is to ensure road safety through the rapid transmission of information to surrounding vehicles. VANET was the first initiative to make communication between vehicles as a reality. It allows to provide V2V or V2I communications through a short-range communication technology. A VANET network consists of 3 elements:

On-Board Unit (OBU): This in-vehicle component allows the vehicle to communicate with surrounding end devices and network devices. The OBU is also used to process information from the vehicle's sensors.

Roadside Unit (RSU): This is a fixed wireless access point located on the road (intersection, parking lot) and designed for vehicle communication. RSU has two main roles. The first is to broadcast information locally (to vehicles directly connected to it and to neighboring RSUs), the RSU is also the Internet gateway for the vehicle with which it communicates.

Central Authority (CA): Allows authentication of vehicles joining the vehicular network (Deeksha et al., 2017).

VANET networks have some limitations that could hinder the development of vehicular network applications. Some of the main limitations include:

The small number of communication types supported: VANET networks rely only on V2V and V2I communications. Therefore, they do not allow the integration of new types of connected objects: cameras, phones, etc. This could limit the effectiveness of various applications such as pedestrian detection.

Limited Internet connectivity: the VANET architecture does not guarantee Internet connectivity to road users. Indeed, due to the low number of RSUs deployed, few vehicles could benefit from Internet connectivity.

Lack of interoperability: the VANET architecture relies only on short-range communications between vehicles and RSUs. It does not allow the use and interconnection of different communication networks.

Complex data processing: the low Internet connectivity and the limited computing and storage capacities make it impossible to process large volumes of data. Thus, global and "intelligent" decision making is complex (Mendiboure, 2020).

2.2.2 Evolution from VANET to IOV

To address the limitations mentioned above, a new paradigm of vehicular communication, based on VANET, 5G cellular communication technology, and the Internet of Things, has been defined as the Internet of Vehicles (IoV) that was created to improve the capabilities of VANETs and enhance autonomous vehicles by guaranteeing V2X communication, i.e. V2V, V2I (RSU, traffic light or sign), V2P (pedestrian or cyclist) and V2N (communications between a vehicle and a network equipment, generally BS) (Gasmi & Aliouat, 2019).

In an IoV environment, each vehicle is seen as a smart object equipped with sensing platforms, computing facilities, control units and storage, connected to each entity (other vehicles, RSUs, charging/gas stations, cloud, etc.) through the vehicle-to-everything communicates (Shen et al., 2020). Thus, requirements such as high speed, low latency and high reliability of the Internet of Vehicles make 5G an emerging solution to current vehicular network challenges.

The 5G technology supports three types of communication:

enhanced Mobile Broadband (eMMB): to allow ultra-high-speed connection indoors and outdoors, with uniform quality of service, even on the edges of a cell.

Ultra-Reliable and Low-Latency Communications (URLLC): to manage communications with significant latency, reliability and availability constraints. URLLC is particularly intended for vehicular applications (road safety).

Massive Machine Type Communication (MMTC): to allow a very large number of connected devices. The objective of this category is to provide a response to the exponential increase in the density of connected objects (Storck & Duarte-Figueiredo, 2019).

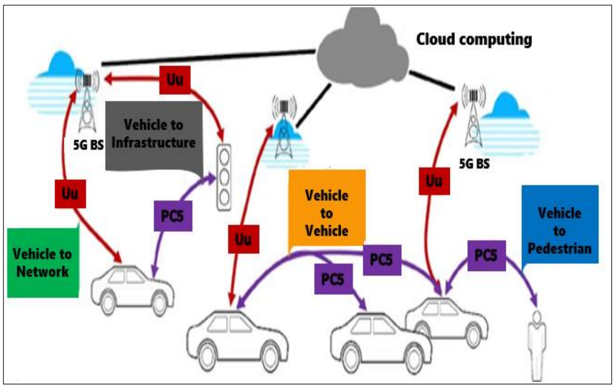

Figure 1. 5G IoV environment

In the 5G IoV environment, communication is provided by the Uu interface which is responsible for connecting vehicles directly to mobile network base stations and supporting V2N services. The PC5 interface which provides V2V, V2I, and V2P applications with high reliability and low latency requirements.
The 5G base station authenticates the vehicles in its coverage area and generates a D2D token to establish direct communication between the vehicles through the pc5 interface (Figure 1). A vehicle that is outside the coverage area of the 5G base station can communicate with another vehicle that is within the coverage area through an ad hoc network that relies on routing protocols to route packets from a source to a destination (Abdel Hakeem et al., 2020).

3 SECURITY ATTACKS IN 5G IOV ENVIRONMENT

In the 5G IoV environment, different attacks on information security and privacy are possible. Attackers can target information such as the vehicle's speed and health, current location and destination route information of vehicles, and the personal information of vehicle users or owners that are stored in infotainment systems (Hoque & Hasan, 2019). Furthermore, due to the wireless medium of the 5G IoV environment, vehicles are open to several types of attacks. In this section we will discuss the most relevant attacks such as eavesdropping, DDoS, Man-in-the-middle, etc.

3.1 Man-in-the-Middle Attacks

Attackers or hackers attempt to access and intercept communications between two independent parties such as V2V, V2I, V2N and even V2P networks. This can be a dangerous attack in an IoV environment. An attacker in the middle discreetly monitors, captures and effectively controls the communication between the two systems (Miao et al., 2021).

3.2 Eavesdropping Attacks

Eavesdropping is achieved when an attacker gains unauthorized access to vehicle messages or communications. Attackers often take advantage of vehicle networks that are not properly secured to intercept data sent or received. In addition to vehicles, RSUs are sometimes targeted in the IoV environments because they play an important role in relaying traffic information. Data or information is usually not disturbed or altered; attackers often try to access information secretly (El-Rewini et al., 2020).

3.3 DoS and DDoS Attacks

A DoS attack occurs when a functional service or system is unavailable for a period of time due to overloaded capacity or exhausted network resources. A DoS attack is a severe attack that can partially or completely disrupt services or systems in the 5G IoV environment, making infrastructure and services unavailable (Trkulja et al., 2020). On the other hand, a DDoS attack is a sophisticated version of DoS. In a DDoS attack, hackers use a large number of infected systems to attack the targeted systems, which makes detection and defense more difficult compared to DoS attacks that are less complex. Unlike network attacks such as eavesdropping and Man-in-the-middle attacks discussed earlier in this section, DoS and DDoS attackers generally are not attempting to steal or modify information. However, the cost of service unavailability on the victim system makes this type of cyberattack more important when it damages the entire network system (Bendale & Rajesh Prasad, 2018).

3.4 Sybil Attacks

An attacker generates multiple identities and uses each one to send different messages to other vehicles, pedestrians and infrastructure. The goal of Sybil attacks is to trick other vehicles, pedestrians, and infrastructure into believing that messages are coming from different vehicles, causing them to make wrong decisions (Lu et al., 2020).

Figure 2 shows an IoV environment with one Sybil attacker, one victim node, and two Sybil nodes. The Sybil attacker in the red vehicle controls the two Sybil nodes (white vehicles) all at the same time, while traveling on the road, the victim node acts on information received from the Sybil nodes without knowing that the information is deliberately sent from an attacker. The attacker can then send wrong information about the condition or happenings on road just to lure the victim node to change its direction.

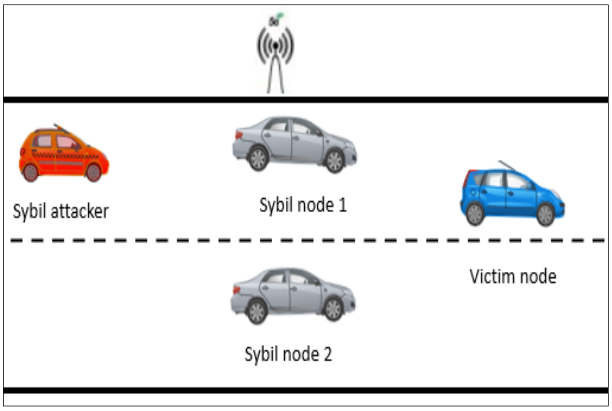

Figure 2. Sybil attack

3.5 Routing Attacks

Routing attacks exploit the vulnerabilities of routing protocols. In these attacks, an attacker can disrupt the normal routing process or drop passing packets. Routing attacks include black hole attacks, grey hole attacks, and wormhole attacks.

A black hole is an area of the network where the network traffic is redirected. Either there is no node in that area or the nodes reside in that area refuse to participate in the network. This causes data packets to be lost. Figure 3 illustrates a black hole attack formed by two malicious red vehicles or nodes, which refuses to forward messages received from legitimate vehicle 1 to legitimate vehicle 2.

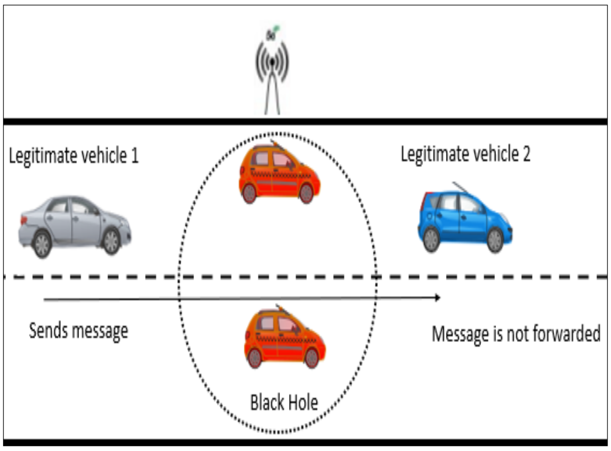

Figure 3. Black hole attack

In a grey hole attack, the attacker selectively drops packets. Additionally, it can switch from correct behaviour to behaviour that performs like a black hole. Due to its occasionally correct behaviour, grey hole attacks are difficult to detect.

In a wormhole attack an intruder catches data packets and forwards them to another malicious node using a wormhole link (a tunnel). This attack is dangerous for avoiding valid routes and losing data packets (Sun et al., 2022).

4 SECURITY SOLUTIONS FOR THE 5G IOV ENVIRONMENT

the following basic security requirements should be satisfied in the 5G internet of autonomous vehicles environment.

Confidentiality: It is designed to prevent disclosure of information to unauthorized entities, so only intended authorized users can access the autonomous vehicle data.

Integrity: It is designed to ensure that the information transmitted is accurate and reliable, and cannot be altered or modified by unauthorized parties.

Authenticity: It aims to confirm the real identity of an entity to distinguish between authorized and unauthorized users.

Availability: It ensures that authorized users can always access autonomous vehicle services on request.

Autonomous Vehicle’s security should be preserved, the information must be kept private and should not be intercepted or revealed to any malicious entity. In this section, we will discuss some solutions or countermeasures to combat attacks from the 5G IoV environment.

4.1 Blockchain

Blockchain is a distributed ledger system that provides a decentralized, reliable and secure solution for sharing information and transactions between parties, instantly and without the intermediary of a centralized authority. The blockchain is composed of a chain of blocks, with the header of the new block containing the hash of the content of the previous block. For this reason, the data and transactions stored on the blockchain ledger are immutable and cannot be changed once they are stored in the ledger. (Zheng et al., 2017). Transaction in the blockchain works as follow.

A vehicle (sender) performs a transaction to another vehicle or any autonomous vehicles component (receiver) which will be signed by its private key. This transaction contains information about the vehicles which can be information about traffic conditions, weather information, or surveillance.

The transaction is validated by the nodes of the network through the verification of the electronic signature on the transaction of the sender. If it is valid and corresponds to his address, using his public key, this transaction will be grouped with other valid transactions in a block.

The block is validated by the nodes of the network using a consensus mechanism that can be proof of work (PoW), proof of stake, proof of authority, etc.

The block is dated and added to the blockchain that all nodes in the network have access to. Each block contains three main elements which are the hash of the previous block, transactions, and the hash of this new block which is calculated through the valid transactions and the hash of the previous block using a hash function.

Finally, the receiver receives the transaction.

4.2 Virtual private network

A VPN creates a tunnel that extends between two endpoints. On one end is a VPN client running on an IoT device in the autonomous vehicle, and on the other end a VPN server running on a dedicated router. These two endpoints add headers to the original packet that contain fields that allow the VPN device to secure the traffic.

The VPN device also encrypts the original IP packet, which means that the contents of the original packet cannot be deciphered by anyone during its transmission over the Internet. Figure 4 below illustrates the VPN tunnel concept (Haga et al., 2020).

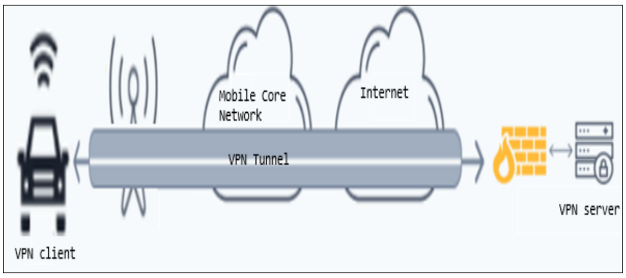

Figure 4. VPN tunnel

4.3 Cryptographic algorithms

Autonomous vehicles contain a great number of devices that transmit data through the 5G IoV network, making this data vulnerable to a variety of security and privacy violations. This necessitates the use of encryption mechanisms to ensure the integrity and confidentiality of information. Thus, the use of cryptographic algorithms can prevent unauthorized access during data storage, processing and sharing (Yang & Johansson, 2020).

4.4 Firewalls and Intrusion Detection Systems (IDS)

Firewalls and IDS are an effective security measures for the internet of vehicles environment. Figure 5 illustrate Firewalls and IDS installed on each vehicle to detect malicious behaviour.

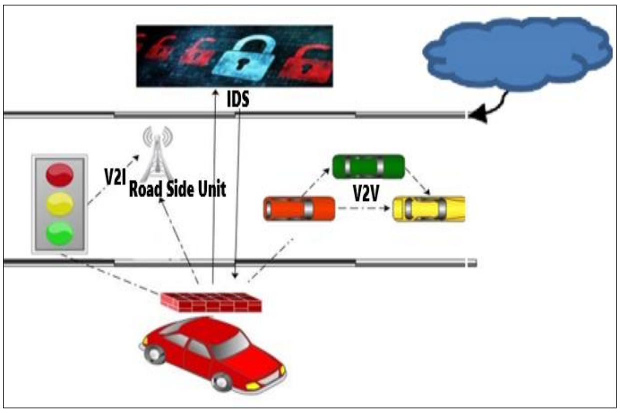

Figure 5. Firewalls and IDS on AVs

A firewall is a network security device that monitors incoming and outgoing network traffic and allows or blocks packets based on a set of security rules. Its purpose is to create a barrier between the internal network and incoming traffic from external sources, such as the Internet, to block malicious traffic (Song, 2020). Also, deploying a network intrusion detection system inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack. An IDS is a detector monitors the cars continuously and detects anomalies. In the IDS data is collected, pre-processed, and anomalies are detected (Ahmad et al., 2018).

5 RESULTS

The security solutions proposed in the previous section are relevant for some attacks and not for others. In this section we will represent the convenient security solutions for each attack (table 1).

Solutions Attacks	Blockchain	VPN	Cryptographic algorithms	Firewalls & IDS
MitM	x	x	x	x
Eavesdropping	x	x	x	x
DoS & DDoS	x	x		
Sybil attack	x			
Routing attacks	x			

Table 1. Solutions for 5G IOV attacks

Blockchain

The data stored on the blockchain cannot be modified because a change in one block will affect the hash of the next block. Also, nodes that do not have the private key associated with the public key distributed in the network cannot perform transactions in place of the owner of the associated address, which makes it possible to resist the Man-in-the-middle attack.

Moreover, with thousands of nodes in the blockchain network, data is available on every node, even if one of the nodes becomes inaccessible, the network will continue to function. Therefore, the blockchain guarantees availability, which makes it possible to resist the DoS and DDoS attacks.

Furthermore, the blockchain allows to anonymize the transactions, which preserves the confidentiality of the data and protects the data from the eavesdropping attack.

Additionally, the consensus mechanism Proof of Work (PoW) can be used to resist the sybil attack. In this mechanism, each identity on the network must perform an equal amount of computing work, thus, each Sybil identity must perform an equal amount of computational work as each honest identity, which makes a Sybil attack too costly because the Sybil attacker requires a higher computational power for each identity created.

Also, the verification of the sender identity and its transaction (in the case of a transaction containing the number of hops to reach the destination is erroneous) allows to resist against Routing attacks.

VPN

The VPN solution encrypts the data sent over the network. This encryption prevents the MITM attack from infiltrating the network traffic. Even if an attacker manages to access the network, the encrypted data blocks him from reading the messages. Therefore, this solution persists against Man-in-the-middle and eavesdropping attacks. One of the main benefits of a VPN is that it hides IP addresses. With a hidden IP address, DDoS attacks cannot locate the network, which makes the target much more difficult. Thus, VPNs can stop DoS and DDoS attacks.

Cryptographic algorithms

As described in the previous section cryptographic algorithms prevent Man-in-the-middle and eavesdropping attacks.

Firewalls and Intrusion Detection Systems

The Intrusion Detection System (IDS) monitors the network and if an attacker tries to hijack the traffic flow, it immediately triggers an alert. On the other hand, Firewalls are the gatekeepers of networks. Thus, IDS and Firewalls prevent Man-in-the-middle and eavesdropping attacks.

6 DISCUSSION

Autonomous vehicles in the 5G Internet of Vehicles environment ensure the safety of its passengers, and road accidents due to human error are significantly reduced. In addition, traffic jams are reduced because the car can detect any future obstacles, making traffic flow more fluid. Also, speed limits can be increased, which would save time for the vehicle's passengers and make driving safer. Additionally, parking is no longer a problem for the driver and passengers, as the car could find a place itself. However, an autonomous vehicle is composed of several sensors (GPS, Radar, Lidar, Cameras, etc.) that are sensitive to several types of attacks named system attacks e.g., GPS spoofing, adversarial Images, radar jamming, etc. We have not addressed this type of attack in this paper as we will deal with it in another work, we are rather limited to autonomous vehicles network attacks (5G IoV environment).

The solutions proposed to deal with these attacks in the 5G Internet of Vehicles environment are relevant in terms of reliability, however, since communication is done in real time in vehicular networks. Response time is a major constraint that can limit the deployment of these solutions.

Considering the example of blockchain, although it is pertinent in terms of reliability, as mentioned in the previous section. The use of current blockchains in the 5G IoV environment has several limitations. Indeed, road safety applications have real time constraints, and the delays induced by the blockchain do not allow them to be respected. Moreover, the performance of current blockchains clearly presents a problem of scalability in terms of the volume of transactions per second: on Bitcoin, a block is only validated every 12 minutes, on Ethereum, it is a block every 30 seconds (Belmannoubi et al., 2020). These numbers are notoriously insufficient if we want to embed blockchain applications in millions of vehicles.

7 CONCLUSION AND FUTURE WORK

This paper presents an overview of the autonomous vehicles and its network. Additionally, the security of the 5G Internet of Vehicles environment is affected by the emerging integration of technologies and intensive communication that lead to an unlimited attack surface. Thus, several 5G IoV environment attacks that can affect confidentiality, integrity, and availability have been investigated, as well as, some security solutions to deal with these cyberattacks.

The proposed solutions to address security attacks in the 5G IoV environment are valid for some attacks and not for others., and they are relevant in terms of reliability, however, the response time is a significant limitation to the deployment of these solutions.

In the future work we will deepen our research on the response time constraint in the proposed solutions and we will focus on system attacks on autonomous vehicles.

REFERENCES

Abdel Hakeem, S. A., Hady, A. A., & Kim, H. (2020). 5G-V2X : Standardization, architecture, use cases, network-slicing, and edge-computing. Wireless Networks, 26(8), 6015-6041. https://doi.org/10.1007/s11276-020-02419-8

Ahangar, M. N., Ahmed, Q. Z., Khan, F. A., & Hafeez, M. (2021). A Survey of Autonomous Vehicles : Enabling Communication Technologies and Challenges. Sensors, 21(3), Art. 3. https://doi.org/10.3390/s21030706

Ahmad, I., Kumar, T., Liyanage, M., Okwuibe, J., Ylianttila, M., & Gurtov, A. (2018). Overview of 5G Security Challenges and Solutions. IEEE Communications Standards Magazine, 2(1), 36-43. https://doi.org/10.1109/MCOMSTD.2018.1700063

Belmannoubi, S., Hadded, M., Touati, H., & Kamoun, F. (2020, novembre). La Technologie Blockchain pour Améliorer la Sécurité des Systèmes de Transport Intelligents. CSTI’20 – 1er Colloque Francophone des Systèmes de Transports Intelligents. https://hal.archives-ouvertes.fr/hal-03000626

Bendale, S. P., & Rajesh Prasad, J. (2018). Security Threats and Challenges in Future Mobile Wireless Networks. 2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN), 146-150. https://doi.org/10.1109/GCWCN.2018.8668635

Bezai, N. E., Medjdoub, B., Al-Habaibeh, A., Chalal, M. L., & Fadli, F. (2021). Future cities and autonomous vehicles : Analysis of the barriers to full adoption. Energy and Built Environment, 2(1), 65-81. https://doi.org/10.1016/j.enbenv.2020.05.002

Deeksha, Kumar, A., & Bansal, M. (2017). A review on VANET security attacks and their countermeasure. 2017 4th International Conference on Signal Processing, Computing and Control (ISPCC), 580-585. https://doi.org/10.1109/ISPCC.2017.8269745

El-Rewini, Z., Sadatsharan, K., Selvaraj, D. F., Plathottam, S. J., & Ranganathan, P. (2020). Cybersecurity challenges in vehicular communications. Vehicular Communications, 23, 100214. https://doi.org/10.1016/j.vehcom.2019.100214

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

Gasmi, R., & Aliouat, M. (2019). Vehicular Ad Hoc NETworks versus Internet of Vehicles—A Comparative View. 2019 International Conference on Networking and Advanced Systems (ICNAS), 1-6. https://doi.org/10.1109/ICNAS.2019.8807870

Haga, S., Esmaeily, A., Kralevska, K., & Gligoroski, D. (2020). 5G Network Slice Isolation with WireGuard and Open Source MANO : A VPNaaS Proof-of-Concept. 2020 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), 181-187. https://doi.org/10.1109/NFV-SDN50289.2020.9289900

Hoque, M. A., & Hasan, R. (2019). Towards an Analysis of the Architecture, Security, and Privacy Issues in Vehicular Fog Computing. 2019 SoutheastCon, 1-8. https://doi.org/10.1109/SoutheastCon42311.2019.9020476

Lakomicki, P. (2018). Démarche incrémentale pour qualifier la fiabilité du système de perception et de décision du véhicule autonome [Phdthesis, Université de Technologie de Troyes]. https://tel.archives-ouvertes.fr/tel-03612974

Lu, R., Zhang, L., Ni, J., & Fang, Y. (2020). 5G Vehicle-to-Everything Services : Gearing Up for Security and Privacy. Proceedings of the IEEE, 108(2), 373-389. https://doi.org/10.1109/JPROC.2019.2948302

Mendiboure, L. (2020). Distribution géographique de données dans l'Internet des Véhicules : Une approche logicielle et sécurisée utilisant les réseaux cellulaires [Phdthesis, Université de Bordeaux]. https://tel.archives-ouvertes.fr/tel-02985383

Miao, J., Wang, Z., Miao, X., & Xing, L. (2021). A Secure and Efficient Lightweight Vehicle Group Authentication Protocol in 5G Networks. Wireless Communications and Mobile Computing, 2021, e4079092. https://doi.org/10.1155/2021/4079092

Pham, M., & Xiong, K. (2021). A survey on security attacks and defense techniques for connected and autonomous vehicles. Computers & Security, 109, 102269. https://doi.org/10.1016/j.cose.2021.102269

Shen, X., Fantacci, R., & Chen, S. (2020). Internet of Vehicles [Scanning the Issue]. Proceedings of the IEEE, 108(2), 242-245. https://doi.org/10.1109/JPROC.2020.2964107

Song, X. (2020). Firewall Technology in Computer Network Security in 5G Environment. Journal of Physics: Conference Series, 1544(1), 012090. https://doi.org/10.1088/1742-6596/1544/1/012090

Storck, C. R., & Duarte-Figueiredo, F. (2019). A 5G V2X Ecosystem Providing Internet of Vehicles. Sensors, 19(3), Art. 3. https://doi.org/10.3390/s19030550

Sun, X., Yu, F. R., & Zhang, P. (2022). A Survey on Cyber-Security of Connected and Autonomous Vehicles (CAVs). IEEE Transactions on Intelligent Transportation Systems, 23(7), 6240-6259. https://doi.org/10.1109/TITS.2021.3085297

Trkulja, N., Starobinski, D., & Berry, R. A. (2020). Denial-of-Service Attacks on C-V2X Networks (arXiv:2010.13725). arXiv. https://doi.org/10.48550/arXiv.2010.13725

Yang, J., & Johansson, T. (2020). An overview of cryptographic primitives for possible use in 5G and beyond. Science China Information Sciences, 63(12), 220301. https://doi.org/10.1007/s11432-019-2907-4

Zanchin, B. C., Adamshuk, R., Santos, M. M., & Collazos, K. S. (2017). On the instrumentation and classification of autonomous cars. 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC), 2631-2636. https://doi.org/10.1109/SMC.2017.8123022

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology : Architecture, Consensus, and Future Trends. 2017 IEEE International Congress on Big Data (BigData Congress), 557-564. https://doi.org/10.1109/BigDataCongress.2017.85