International Journal on Cybernetics & Informatics (IJCI) Vol.13, No.2, April 2024

Advancements and Hurdles in the Evolution of Automotive Wireless Interfaces: A Technical Exploration

Nuha Sabek , Joseph Loftus , Kati Sneath , Spencer Ames , and Tauheed Khan Mohd

School of Information Security and Applied Computing, Eastern Michigan University, Ypsilanti, Michigan, USA

Abstract. The integration of wireless interfaces into vehicles has posed some challenges for the automotive industry over the years. While manufacturers strive to impress consumers with cutting-edge features, these features also bring security risks that cannot be ignored. To prevent potentially fatal incidents, a thorough protocol must be established to address system vulnerabilities. As the modern century moves towards an era of autonomous vehicles, security must be a top priority to avoid compliance breaches and delays in feature development. The significance of vehicle interfaces in the modern automotive industry cannot be overstated.

The present study aims to explore the prospective advantages and challenges associated with the integration of wireless interfaces in the automotive industry. This analysis will primarily focus on the latest technological advancements in vehicle technology and the critical need to secure against possible cyber-attacks. A wide range of topics will be covered in this paper, from the evolution of vehicle interfaces to the industry's hurdles and strategies to minimize the risks associated with cyber threats. The objective of this study is to provide a comprehensive understanding of wireless interfaces in the automotive sector, including the benefits of implementing such technology, the challenges that it poses, and the measures needed to maintain the security and safety of vehicles, as well as the passengers.

Keywords: Vehicle Interfaces · Vehicular networks · Evolution of vehicle interfaces · Automotive cybersecurity · vehicle safety · technology of the future

1 Introduction

Vehicles have come a long way from the beginning of time when the only options were basic features (steering wheel, accelerator, and brakes)[1]. Currently, a majority of cars today include some sort of wireless interface that assists the driver. These wireless interfaces can be very complex like the electronic control units

Bibhu Dash et al: NLPAI, IOTBC, CITE -2024
pp. 149-159, 2024. IJCI – 2024
DOI:10.5121/ijci.2024.130211

but as simple as keyless entry. Some of the major selling features of cars today are the options offered to make the user's experience better. The most popular options to ensure the car comes equipped with include Bluetooth, WIFI, electric car start, and a GPS navigation system. These four options are what will allow a user to listen to music, talk on the phone hands-free, start the car from the comfort of the user's own home, and find the fastest route to the destination without road delays. Most cars today have all these features which do not make any of these components stand out from the rest. Manufacturers all around are trying to find the next best thing to ensure that future cars produced include features that fit the current user's needs.

As the world of cars evolves into the future, vehicle options are only getting more complex. The Automotive Internet of Things is evolving into making cars become its own highly intelligent entity. Automotive IoT is a complex system that is built up of sensors, cameras, and trackers that are connected to the cloud to offer cars all its wireless features. These sensors and cameras are not only inside the car but also placed outside to offer some features like assistance with backing up or alerting you when a vehicle or person is behind the car. Currently, the modern vehicle is called a "computer on wheels" [2]. The reality of autonomous cars driving on its own, while the user is a passenger, is right around the corner, however, this concept opens the possibilities to more vulnerabilities.

Since everything is going to computer technology, including cars, this leaves room for security risks to happen [3]. Strong security measures need to be put into place to make sure all the added features are working properly, and any updates are implemented to avoid the possibility of attacks. Using security techniques that were traditionally used with computers, such as two-factor authentication and biometrics, or needing to develop whole new technologies and understandings of security might be needed to better secure vehicles and different wireless interface systems. Currently, vehicles consist of 50-70 electric control units (ECUs). It is important to make sure the firmware is updated or it could result in an attack [4]. Should an attack happen, it could destroy any of the major vehicle manufacturers or cause great financial loss.

With all this information and how technical vehicles are becoming, it will take a large security team that is experienced with this type of technology to keep up. Without a good team to make the moving parts work to keep the vulnerabilities at a low, these technologies could cause more issues as the current era moves into the future of cars. If the vulnerability levels can stay within the low range, the future is looking bright for the automotive world. This paper will go into detail about all of these different topics to give a better understanding of what is involved with the evolution of vehicles to get these automobiles to be where the industry is giving the end user the interfaces of tomorrow while keeping it all secure from attacks.

2 Related Work

With the rise of technology, automation within vehicles has additionally risen significantly. This is prominently seen with wireless interfaces within vehicles and, currently, the significant amelioration of autonomous vehicles. The mitigation of autonomous and wireless vehicles sheds light on the vast and continuous pace that occurs. These meliorations are present more prominently in autonomous vehicles.

Autonomous vehicles demonstrate multiple attack vectors due to their increased virtualization. These attack vectors are autonomous control systems, autonomous driving system components, and vehicle-to-everything communications. An example, autonomous vehicles may include highly developed software that the modern vehicle may be deficient in, such as automatic brakes. A hacker that breaks into the computer software of these autonomous vehicles, would have the ability to create infinite damage, including stopping the car engine, disabling the brakes, remote controlling said vehicle, taking control of the accelerator/speed, identity theft from phone connectivity to car software, hacking the USB port, etc. These attack vectors create numerous openings for vulnerabilities.

While one may believe the modern vehicle interface is safe from hackers, this statement proves to be false. Modern vehicles have multiple vehicle attack vectors that include: Wireless Bluetooth, Cellular, Key Fob, Satellite Radio, Reverse Camera, Blackbox, Visual Sensors, Radar, Lidar, Sonar, Tire Pressure Monitoring Systems, etc. These attack vectors are present in many modern vehicles. These attack vectors are a gateway for hackers to interject and cause fatal damage to the vehicle and operator of that vehicle. Similar to autonomous vehicles, these attack vectors create multiple possibilities of several vulnerabilities.

To go into further detail, one can look to a more modern tool that comes with all newer cars; the key fob. Key fobs provide the owner of the car with the ability to control certain aspects of the car, such as the door locks, emergency horn, and the trunk, from a distance. Additionally, key fobs come with transponders located inside the device that can act as a security tool, with the intention of not allowing the car to start if the key fob is not located nearby [5].

When implemented properly, those security features can prevent older forms of theft, such as hot-wiring a vehicle. When not implemented correctly, these features serve no benefit to the security of the vehicle. In recent times, thieves have been able to steal certain cars that still use keyed ignitions, and not push-to-start vehicles, with just a USB stick. There is no hacking even taking place in this situation, the USB just had the proper dimensions needed to turn the ignition. The reason these vehicle thefts have been taking place is that the cars lack the use of a transponder with their key fob, so the vehicle itself is not what is similar to a two-factor authentication system to keep the car secure.

Just to show how even though the evolution of the systems of the vehicle can bring positives, there will always be a downside, no matter how hard security specialists try to keep things safe. Even though the key fob can bring positives in overall usability and security to the vehicle, hackers and criminals are developing techniques just as fast to exploit this device. For example, the key fob is

vulnerable to relay attacks, such as signal boosting. Attackers can use a radio transmitter to boost the radio signals sent from the key fob, thus allowing the threat actor to trick the vehicle in which the fob is nearby, allowing the attackers to unlock the vehicle.

Just with the example of the key fob alone, one can see that there are both positive and negative effects of introducing newer and more technical utilities within the vehicle. Keeping that in mind, security teams must play a key role in the development of these systems, in order to maintain the highest level of security for the vehicle, to keep the vehicle, and therefore the passengers of said vehicle, safe at all times.

While vehicles are like a computer that sends and receives data, what could keep an intruder out? The same concept as a computer is to have a firewall or an IDS (intrusion detection system). The idea is to have a monitor of incoming packets. This would need to be updated regularly to keep up with the latest threats. The amount of interconnected data will depend on what the vehicle is capable of or the system components it is using. Now vehicles will send remote diagnostics through the ECU which is essentially the vehicles' computer. Utilizing the Onboard Diagnostics that are connected to the vehicle's PCM (Powertrain Control Module) and ECM (Engine Control Module) which is interchangeable with ECU or Engine Control Unit. As of this writing, these are still in effect with ICE vehicles or internal combustion engines. The PCM and ECM all communicate via a 5-volt reference signal. This reference signal is what tells the vehicle's ECU what is happening at that sensor. The reference is all registered to the OBDII which has preset ranges for each of the vehicle's sensors to navigate how the engine or powertrain is doing. Briefly, the sensors a vehicle has are oxygen sensor, parking, throttle position, manifold absolute pressure, camshaft position, engine speed, TPMS (Tire Pressure Monitoring System) and the list goes on. The simple reason to talk about vehicle systems is to understand what is under attack. Currently, there is a transition to BEVs or EVs that does not change how a vehicle can be attacked other than there is less need for so many sensors without an engine. For now, the focus can be on what is more prevalent on the roadways and that is ICE (internal combustion engine) vehicles.

Knowing a brief introduction to what a vehicle has controlling normal operations will help manufacturers understand what vulnerabilities it has. If there is a way to attack a vehicle wirelessly it is a guarantee that the entity responsible will have access to the most vital components of a vehicle. The vehicle relies on so many components in the loop to operate and just getting access to some of these loops would be detrimental. Imagine getting into a car knowing what has just been described above about the systems on a vehicle. The attacker could debilitate the vehicle as the attack vectors are not fully secure. If the vehicle has all the information about the systems going to the control modules and the onboard diagnostics an attacker can see this information. Before vehicles used Wi-Fi this information would be unavailable. OBDII via Wi-Fi can be attacked through an interface like the infotainment system in Fiat Chrysler Automobiles or FCA. There are three protocols LIN (Local Interconnect Network), CAN (Controller

Area Network), and FlexRay that can be used to gain access to a vehicle's ECU. Lin is used to communicate between the different control units within a vehicle's system [6].

Finding a way to get into the CAN and knowing what protocols are in place will give the attacker a leg up in knowing what codes are represented by certain components in the vehicle's interface. Unfortunately, CAN has been around since the 80's. The technology, environment, speed of communication, and/or type have developed in more recently. The continued use of CAN is simple as it comes down to cost. CAN is a cost-effective way for manufacturers to complete vehicle system communications. Using older technology with more advanced technology creates vulnerabilities because the CAN protocol does not have security features [6]. As mentioned above the Tire Pressure Monitoring System can be another avenue of attack as you could decode the signal that it sends to the ECU. This same attack can be used with the key fob to copy the signal it is sending remotely. These are simple examples of attacks on the CAN bus utilizing the sensor as the vulnerability. As time goes on the vulnerabilities will have to be secured in some way. Maybe the TPMS that uses a UHF (Ultra High Frequency) and low-frequency signal, depending on the vehicle, will have to find another avenue of communication. The TPMS signal can be replicated by the same radio frequency by creating a tool that would allow the same frequency to register with the vehicle's ECU. The attacker could even register the device as a known TPMS sensor while having access to the ECU. The entire point of accessing the ECU is to give access to all the system components to own it. Technology allows devices to send signals remotely while giving vulnerabilities at the same time.

3 Research/Findings

The evolution of vehicles has come a long way as cars have become smart, intelligent, and connected [7]. Back in the 80s, only 1 percent had electronic equipment and in the modern era are at a 50 percent increase currently. Vehicles today are built of a complex system that is made up of 100 million lines of code making it computer-like over mechanical [8]. Modern vehicles can communicate both internally and externally with the different networks in place. An in-vehicle network has been put into place to assist with the communication of all the ECUs. Within the in-vehicle network, automotive bus systems enable ECUs to communicate with one another and with other subsystems. The ECUs are mostly responsible for all actions of the car. These ECUs control small actions like opening the windows all the way to the larger actions like the automatic brake system.

Within the in-vehicle network, there are also protocols. There are four that are well-known which consist of CAN, LIN, Most, and FlexRay. Each one of these protocols has a set of actions to perform and communicates back to the gateway. The CAN is responsible for critical communications with managing the engine, communicating with the body, and making sure the airbags deploy when triggered. The Controller Area Network (CAN) bus protocol is a method of communication used to send messages to Electronic Control Units (ECUs)

that prompt sensors to respond appropriately. This methodology ensures that the system operates efficiently and accurately. The CAN bus protocol system is responsible for transmitting messages to the corresponding ECUs, which then prompt the appropriate sensors to respond. This communication methodology is vital for the proper functioning of the system. It enables communication between various parts of the system, allowing for the transmission of data between the ECUs and sensors. Due to its ability to transmit data quickly and efficiently, the CAN bus protocol system is widely used in modern vehicles. LIN controls the internal components like door locks, seat belts, lighting, windows, and mirrors. The last well-known protocol is FlexRay. FlexRay is a multimedia protocol that is faster but also more expensive. It oversees multimedia and x-by-wire [7]. The in-vehicle network also has a gateway. This gateway is how external components can access the ECUs to run tests or diagnostics remotely.

Since all ECUs have their own firmware, it is detrimental for engineers to be able to run diagnostic tests on the ECUs to find out if there are bugs that need patches. This allows the engineers to research the car to find out why it is not performing correctly. The engineers can then deploy a firmware solution. Typically these solutions are deployed over the air (FOTA) [9]. The FOTA approach is very beneficial to manufacturers today because it allows the service to send updates without inconveniencing the customer, the updates are downloaded right away over a wireless network connection from a trusted portal and dispersed to the correct ECU. Once the system has rebooted, it should perform better with the new functions that were deployed [9]. Ensuring security is crucial when it comes to the Electronic Control Units (ECUs) of a vehicle. These units are responsible for the proper functioning of a vehicle, and therefore, it is the responsibility of the developers to ensure that the deployment of these units is secure and free from vulnerabilities. Software attacks pose a significant threat to embedded systems, which can ultimately put the customers at risk.

Since there are so many moving parts in modern vehicles, the risk of vulnerabilities has gone up. These systems have created more opportunities for hackers to steal control of a vehicle to cause risk. All it takes is the attacker to hack the system and take control of the consumer's vehicle.

To better mitigate the threat of attackers that could gain control of a user's vehicle, research was conducted by the Department of Computer Science and Engineering at Chalmers University of Technology. In an attempt to understand the "view" of an attacker, the researchers involved assumed that an attacker has access to the "wireless communication link" to perform cyber attacks on a vehicle [10]. The Dolev-Yao attacker model was adopted. It's where an attacker can eavesdrop, intercept, modify, and inject messages into the communication link. Therefore, it was found that the attacker mainly aimed to disrupt the connection between the automotive manufacturer and the vehicle [10]. By doing so, the attacker could cause the communication to fail or even modify the "messages" to effectuate arbitrary actions.

Further discussion of the damages inflicted by attackers using the model previously discussed. An attacker could toy with the "remote diagnostics", modify-

ing the read and control requests, causing it to fail. Same way, flipped around - the attacker could inject read and control "messages" to perform arbitrary actions. These arbitrary actions are confined to the performance of the correlation of the ECU. [10].

If an attacker gains access to or messes with the ECU of a vehicle, then the attacker can gain control over critical vehicle functions, compromising the safety of the user/driver. An example would be if the attacker compromises the ECU controlling the breaks, then the attacker could disable the brake abilities or apply the brakes, harming the driver/user at hand. This is one example of many in how an attacker could cause harm through access to the ECU.

While the ECU of a vehicle is essential in mitigation techniques, there are other features of a vehicle that leave it vulnerable to attacks, and further analysis is required. This would be the Bluetooth feature of a vehicle. Similar to the ECU, Bluetooth has evolved and merged its way into modern vehicles, improving constantly [11]. Although Bluetooth was developed in 1994, it has come a long way since its integration in vehicles [12]. With its development, it brings on more vulnerabilities and threats from attackers.

Bluetooth/wireless interfaces within vehicles arise with complications, according to research [13]. The complication was that there are several challenges in securing wireless interface vehicles [13]. Any security mechanism will require "additional processing overhead, and on the hardware level, has ramifications in the provision of energy and in physical assembly and design, such as placement of additional wiring" [13]. However, if these changes were possible/addressed, the defenses at the software level, such as cryptography, intrusion detection systems (IDS), and firewalls cannot be implemented without considerable changes to the architecture due to different protocols and "topologies" within the automotive domain. Even once a vehicle has been sold, patches for any discovered vulnerabilities after release can be difficult. [13].

Additionally, each Bluetooth implementation process differs from the other. One way this can be identified is through the pairing process. Bluetooth utilizes two pairing processes: Legacy pairing and SSP. [13]. One of the two following processes is used to link a device to a host via Bluetooth. Arising back to the vulnerabilities and threats identified with Bluetooth, there are multiple vulnerabilities associated with Bluetooth. Some of these vulnerabilities include Man-in-the-Middle attacks, unauthorized direct data access, malware, denial of service attacks, sniffing, obfuscation, fuzzing, range extension, and surveillance [13]. There are many categories of attacks that could be performed. Each attack listed conveys a trend that plays an important part in identifying the end goals of an attacker.

Additionally, attacks on the sensors of more modern vehicles can make for very serious problems, especially if the attacks target self-driving vehicles. Self-driving vehicles require a multitude of different sensors, technology, and logic to allow the automobile to operate safely on the roads. "Many of the inputs utilized by autonomous vehicle systems are based on already present sensors and systems. These signals are readily available on the vehicle's CAN and are utilized to

provide vehicle information and are also utilized to generate responses based on autonomous vehicle sensors outputs." [14] Varghese lists the input devices being used by these vehicles: Wheel speed sensor, Yaw rate sensor, Lateral/ Longitudinal sensors, Steering Inputs, Hydraulic Brake Boosters/Hydraulic Pump, Driver inputs, Transmission outputs, Powertrain outputs, Powertrain outputs, HMI. As mentioned previously, an attacker could try and take out or manipulate the braking system in these cars. This can be especially dangerous when the driver of the vehicle has not been operating the vehicle manually and has not had the chance to physically test the brakes in some time. Another example is attacking the tire pressure sensors through the CAN system, causing the vehicle to think that the tires have gone flat, then advising the driver to pull over and assess the vehicle. At that point, the attacker could follow the victim, and could be free to commit many other crimes against said victim. Attacks like these are reasons why the automotive and cybersecurity industries need to ensure the constant updating and hardening of these systems, especially with the evergrowing technological development that is the world of autonomous vehicles.

An extremely important portion of the functionality of the vehicle is its Global Positioning System (GPS). The GPS can give vital information to a driver, such as the driver's current location, directions to a requested destination, the local speed limit the driver must abide by, recent accidents that may have occurred in the area, and information on road work. Going even further in autonomous vehicles, lane support systems use GPS as a vital component. Lane support systems are " Any systems that aids in helping the driver stay in his or her lane. This is generally done utilizing vision systems or GPS."[14]. The GPS will always be essential to the core functions of the automobile, thus attackers must not have the ability to disable or misappropriate the information coming and going from this system.

One of the examples of CAN bus attacks via Bluetooth briefly commented on earlier was a fuzzing attack. Fuzzing is the process of loading the CAN bus with messages to see what responds or gets through to the ECUs. The attacker can monitor how the CAN fuzzing changes what the vehicle's instrument display is showing or the IVI (in-vehicle infotainment) or any other changes in the CAN bus payload. The ECUs reaction to the fuzzing attack can allow the attacker access to the ECU. Another attack on the vehicle CAN bus is the ECU impersonation attack. If the attacker can impersonate the ECUs, then the threat actor has a front-row seat to the traffic on the CAN bus to monitor. The attacker can learn what traffic is controlling which ECU which then can be replicated to impersonate a particular or multiple ECUs. The attack uses the CAN ID while monitoring the frequency to repeat later to take control of any ECU on the CAN bus that is replicated. When attacked ECU sent a recessive bit while the attacker sends a dominant bit this leads the ECU controller to remove it from the bus due to the error it causes thus allowing the attacker to still listen without being seen because the ECU is dropped off the bus. Injection of data into the CAN bus faster than normal and without authentication the attacker can manipulate the behavior of the data on bus to create an event that allows the attacker to take

control create events. This injection attack can seem legitimate while gaining control of an intended mark on the CAN bus [6].

The CAN bus is sending and receiving bus frames that are not authenticated. This lack of authentication allows the can bus to be vulnerable to attacks using frame injection. Authentication not being present allows for sniffing, for example using CarShark software to scan and examine the traffic. One important thing to remember is that loading the CAN bus with larger encrypted payloads can affect the transmission time. The attackers know that vulnerabilities will be there due to the nature of the CAN bus and how it must be effectively fast to make the vehicle safe [6]. There lies the possibility of vulnerabilities due to the nature of vehicle communication requiring speed for safety. The nodes on a vehicle network are not segmented which simply means that every node is linked to the same bus. The network sends and receives messages that each node can see allowing the attack to see the nodes on the CAN bus [6].

The attack on the CAN network can be simple to complex depending on the vehicle's security/IDS, encryption, and how well the manufacturer Fuzz tested the vehicle prior to release. Today with vlogs, forums, and just running a search on the internet it's not hard to learn about how to penetrate the vehicle's wireless systems. An interesting way to dive into CAN communication on the bus is the use of diagnostic tools. Sniffing the traffic while the diagnostic tool is talking to specific ECUs. According to Li et al., diagnostic tools can communicate with the ECUs by putting the "ECU into a diagnostic mode, preventing the device from communicating on the CAN bus" [15]. This is like what was described earlier how an attacker can take the ECU of the can bus and just listen to the network communications to learn what packets are being sent. Also, once the ECU is obtained the attacker can figure out the details of the ECU chip by finding the chip's model number. Once the model number is obtained the reverse engineering can be acquired by researching the chip through various online searches. However, this might not always be the case and the attacker is going to have to go deeper into the vehicle's systems. If the attacker can gain access to the vehicle's control module to find the firmware, the threat actor can try to reverse it. By reversing the ECUs firmware, the attacker can figure out what data belongs to what functions to perform specific actions [15].

Conclusion

The vehicle has come a long way since the beginning of time. Vehicles have been upgraded to serve what post-modern automobiles could not feature, which include the integration of wireless interfaces and the vehicle's ECU. Each provides a vast and greater experience for users. With Bluetooth, Wi-Fi, electric car start, GPS navigation, and future automation, multiple attack vectors were demonstrated due to increased virtualization. Hackers' knowledge and substantial ability to find the vulnerabilities and vectors in these wireless interfaces prove fatal to the vehicle or the consumer. Cyber-attacks on the ECU or CAN bus can be simple or complex, granting hackers control over vehicles and posing

serious risks to consumers. Hackers need only to sniff traffic during vehicle wireless updates to access important information, which can be used to hack into the system. To prevent this, manufacturers must ensure that the platform used for updates is secure and updated, leaving no vulnerabilities for hackers to exploit. Research has demonstrated that certain factors and vectors can be utilized to effectively mitigate security threats to modern vehicles. While implementing these mitigation techniques is crucial to safeguarding vehicles, it is equally important for researchers and developers to have a comprehensive understanding of the threat model from the perspective of hackers. By adopting a hacker's point of view, researchers can more effectively develop solutions that address potential vulnerabilities and enhance the overall security of modern vehicles.

Future Work

Extensive research has revealed numerous promising areas for enhancing vehicle interfaces in the automotive industry. The primary focus of this exploration was the evolution of vehicle interfaces and the implementation of security protocols. The results of this comprehensive analysis indicate that there is ample potential for further research and development on vehicle interfaces and keeping it safe. To address concerns regarding the security of vehicle interfaces, several viable avenues for further research have been identified:

- Analyze the security protocols currently in place for vehicle interfaces and identify any potential weaknesses.
- Investigate any known weaknesses or breaches that manufacturers are currently encountering with the CAN bus and ECU systems.
- Construct a compelling and concise case for the importance of continued research and advancement in this field.
- Conclude with actionable suggestions for future research and development, highlighting potential focal points and the essential resources required.

After concluding this research plan, manufacturers will have a better understanding of how to improve interface technology to avoid leaving consumers vulnerable to security issues. Research is a ongoing process from initial problem, to development, and finally implementation.

References

1. S. Damiani, E. Deregibus, and L. Andreone, "Driver-vehicle interfaces and interaction: where are they going?," 2009.
2. D. Klinedinst and C. King, "On board diagnostics: Risks and vulnerabilities of the connected vehicle," *CERT Coordination Center, Tech. Rep*, 2016.
3. K. Han, A. Weimerskirch, and K. G. Shin, "Automotive cybersecurity for in-vehicle communication," *IQT QUARTERLY*, vol. 6, no. 1, pp. 22–25, 2014.
4. D. K. Nilsson and U. Larson, "A defense-in-depth approach to securing the wireless vehicle infrastructure.," *J. Networks*, vol. 4, no. 7, pp. 552–564, 2009.

5. C. Hodge, K. Hauck, S. Gupta, and J. C. Bennett, "Vehicle cybersecurity threats and mitigation approaches," tech. rep., National Renewable Energy Lab.(NREL), Golden, CO (United States), 2019.
6. E. Aliwa, O. Rana, C. Perera, and P. Burnap, "Cyberattacks and countermeasures for in-vehicle networks," *ACM Computing Surveys (CSUR)*, vol. 54, no. 1, pp. 1–37, 2021.
7. H. M. Song, H. R. Kim, and H. K. Kim, "Intrusion detection system based on the analysis of time intervals of can messages for in-vehicle network," in *2016 international conference on information networking (ICOIN)*, pp. 63–68, IEEE, 2016.
8. Z. El-Rewini, K. Sadatsharan, D. F. Selvaraj, S. J. Plathottam, and P. Ranganathan, "Cybersecurity challenges in vehicular communications," *Vehicular Communications*, vol. 23, p. 100214, 2020.
9. D. K. Nilsson, L. Sun, and T. Nakajima, "A framework for self-verification of firmware updates over the air in vehicle ecus," in *2008 IEEE Globecom Workshops*, pp. 1–5, IEEE, 2008.
10. D. K. Nilsson, P. H. Phung, and U. E. Larson, "Vehicle ecu classification based on safety-security characteristics," in *IET Road Transport Information and Control-RTIC 2008 and ITS United Kingdom Members' Conference*, pp. 1–7, IET, 2008.
11. H. Yang, Y. Wang, and R. Jia, "Dimensional evolution of intelligent cars human-machine interface considering take-over performance and drivers' perception on urban roads," *Complexity*, vol. 2020, pp. 1–13, 2020.
12. H. Mamdouhi, S. Khatun, and J. Zarrin, "Bluetooth wireless monitoring, managing and control for inter vehicle in vehicular ad-hoc networks," *Journal of Computer Science*, vol. 5, no. 12, pp. 922–929, 2009.
13. M. Cheah, S. A. Shaikh, O. Haas, and A. Ruddle, "Towards a systematic security evaluation of the automotive bluetooth interface," *Vehicular Communications*, vol. 9, pp. 8–18, 2017.
14. J. Z. Varghese, R. G. Boone, *et al.*, "Overview of autonomous vehicle sensors and systems," in *International Conference on Operations Excellence and Service Engineering*, vol. 2015, sn, 2015.
15. X. Li, Y. Yu, G. Sun, and K. Chen, "Connected vehicles' security from the perspective of the in-vehicle network," *IEEE Network*, vol. 32, no. 3, pp. 58–63, 2018.