Irish Interdisciplinary Journal of Science & Research (IIJSR)
Vol 6, Iss 4, Pages 70-86, October-December 2022

# Investigations on Cybersecurity Challenges and Mitigation Strategies in Intelligent transport systems

Dr. Vinod Varma Vegesna*

*Sr. IT Security Risk Analyst, The Auto Club Group, United States of America. Email: vinodvarmava@gmail.com**

*DOI: https://doi.org/10.46759/IIJSR.2022.6409*

*Article Received: 22 November 2022 Article Accepted: 29 December 2022 Article Published: 31 December 2022*

## ABSTRACT

*Automobiles are becoming more linked, also with the ability to synchronize to cellular telephones, offer atmospheric as well as navigational alerts for vehicle passengers, and even broadcast safety alerts to all other automobiles and nearby infrastructures. Although automobile connectivity or digitalization provides obvious benefits to passenger satisfaction including accident prevention, these have indeed increased potential enabling attackers to take over automobiles that endanger either driver's or pedestrians' life. Since the attackers are capable of hacking vehicular communications, some of the notable automobile attacks became effective. This study expands on discussions about cybersecurity problems concerning cybersecurity challenges and mitigation strategies in intelligent transport systems as well as vehicle communications.*

***Keywords**: Cybersecurity; Cybersecurity challenges; Vehicular communications; Vehicle-to-infrastructure.*

## 1. INTRODUCTION

Intelligent transport systems employ the processing of data, communications, and sensing technologies to cars, infrastructural components, as well as roadside customers to enhance transport system effectiveness and safety [1-8]. Figure 1 depicts the heterogeneity channel's two primary sub-networks: (i) An intra-vehicle system consists of a number of sensors positioned inside the vehicles. Interfaces between devices are facilitated via Ethernet, ZigBee, or WiFi connectivity, (ii) The inter-vehicle network handles communication between the automobile as well as its surroundings. It is consisting of four elements, which are as described in the following: The key component in an intelligent system of transportation is the vehicle's built-in unit. Every automobile is outfitted with a built-in device that can analyze acquired information and communicate with nearby elements.

For the linked entities, V2X offers a standard connection framework. Furthermore, it enables roadway elements to convey information including their present speeds, location, and orientation to both stationary and traveling neighbors. They then utilize this information to arrive at sound judgments. The kind of communication is determined by the entities that form the relationship.

It enables five different communication methods: Vehicle-to-Sensors (V2S) is the interaction among sensing devices inside an intra-vehicle sub-network; Vehicle-to-Vehicle (V2V) is the interaction among automobiles by using V2V implementation; Vehicle-to-Pedestrian (V2P) is the link between both the driver and roadways pedestrians using V2V implementation; Vehicle-to-Grid (V2G) is the interaction among automobiles as well as the power infrastructure to start charging Electric Vehicles. (v) Vehicle-to-Infrastructure (V2I) communication refers to the exchange of information among roadway vehicles as well as infrastructure elements.

As a consequence of technological advancements in sensors including networking technologies, intelligent transportation networks enable the existence of a wide range of applications that concern safety, congestion, as well as navigation systems: (i) Security applications leverage cellular connections across nearby organizations to make the roads safer and keep passengers secure. Every highway object transmits safe communication to its neighbors on a regular basis to reflect its present state. It might also be required to provide an alert message whenever a regional or global incident is identified. (ii) Traffic-related applications are employed in order to effectively control congestion as well as guarantee the movement of traffic. These are already in charge of gathering traffic data and remotely relaying it to a distant computer for assessment. The analytical results are then delivered to cars for prospective use.

Cloud technology, embedded systems, and IoT-based models represent significant developments in the creation of sophisticated devices. In response to the growing amount of interconnected cars, the notion of a vehicular ad hoc network (VANET) and internet of vehicles was born (IOV). VANET is a fundamental paradigm for connecting and stimulating automobiles within a specific level; nevertheless, this could analyze and modify worldwide actual information. The network of cars, on the contrary side, is outfitted with connectivity.

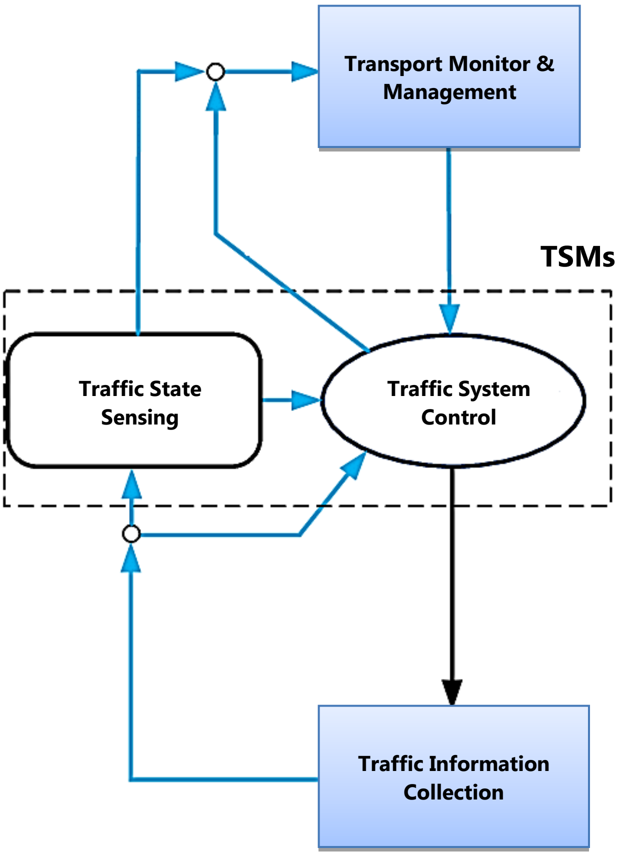
Transport Monitor & Management
TSMs
Traffic State Sensing
Traffic System Control
Traffic Information Collection

**Figure 1.** The architecture of an Intelligent Transportation System

To provide an effective as well as unified framework, IOV incorporates various elements also as individuals, cars, networking, congestion, or paths. The interconnection of cars and also other cyber-physical elements including detectors, the internet, or satellites may offer a worldwide system capable of evaluating all actual information, resulting in a better, more effective, and dependable transport environment.

To proceed, the primary goal of such an SLR is to detect potential vulnerabilities and improve protective measures in IOV. By handling security factors including authorization, the integrity of information, secrecy, end-to-end cryptography, or remote access, a basic protected IOV may be constructed. IOV is very susceptible to hackers; it has been attacked and controlled merely by changing its automobile to computer connectivity, resulting in unfortunate incidents, security breaches, and the loss of extremely critical data. There are additionally additional privacy precautions associated with each tier of IOV. In IOV, a wide variety of assaults are classified based on their characteristics and proportional elements. Figure 2 depicts IOV communications.

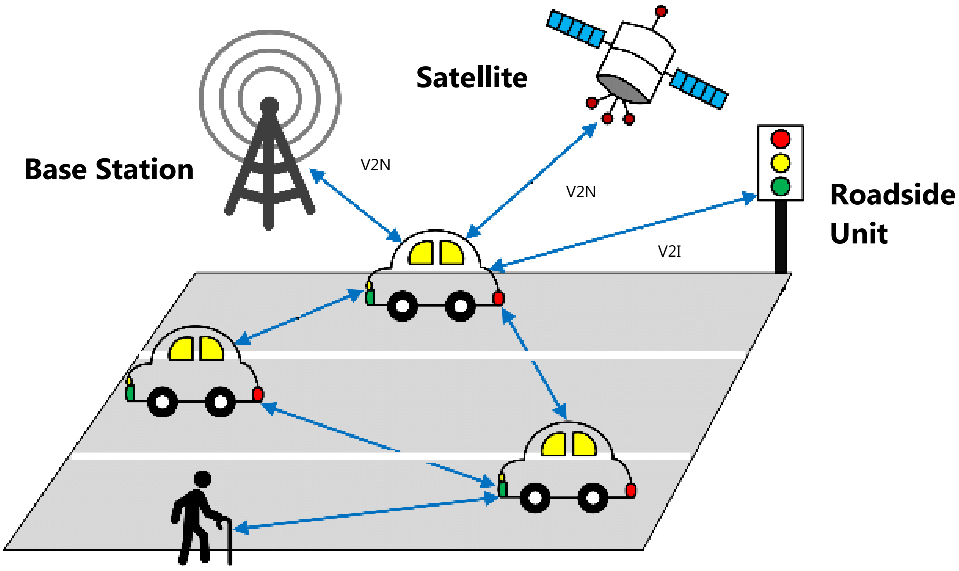

**Figure 2.** Communication in IOV

Because of IoV's broad potential, an increasing number of countries and organizations are researching ways to combine smart transport using conventional modes of transport. These have resulted in an upsurge of unforeseen known vulnerabilities, drawing the issue to the forefront. The United States released Fair Information and Privacy Principles for its Intelligent Transport Systems (ITS) in 1999, and the National Institute of Standards and Technology developed its Cybersecurity Risk Management Framework Applicable to Contemporary Automobiles. Furthermore, the European Union issued its ITS Implementation Plan to restrict the usage of IoV information while ensuring its safety. As a result, the requirement for security precautions in IoV standards would increase even as technology has advanced and thus becomes extensively utilized in the near future. To guarantee that perhaps the IoV platform fulfills safety requirements for users as well as automobile data protection, decentralized, flexible, and robust cybersecurity technologies are required. The Sybil attack has become one of the most popular forms of assault in VANETs and IoV. Researchers studied contemporary primary sources when researching the Sybil attack. A number of approaches have been suggested by different researchers to avoid Sybil attacks in networks. Yet, there is nevertheless room for improvement since the present approaches contain significant downsides, including the reality that many of the recommendations rely on a substantial number of nodes or RSUs.

## 2. THE SEVERAL CATEGORIES OF CYBER ATTACKS

(1) Sybil attack: The Sybil attack has become one of the most popular forms of assault in VANETs and IoV. Researchers studied contemporary primary sources when researching the Sybil attack. A number of techniques have been suggested by various researchers to avoid Cyberattacks in networks [9-14]. Nevertheless, there remains room for growth since the present approaches contain significant downsides, for example, the fact that many of the suggested solutions rely on a huge number of nodes or RSUs.

(2) Denial of service (DOS): Denial of Service (DoS) assaults are likewise regarded as being among the most serious threats, according to research studies. The present security techniques for DoS attacks include fundamental flaws: Some suggested alternatives depend on human parameter selection, which would be impractical, and base stations are also not identified in certain existing frameworks if the system is overwhelmed with fake information. As a result, despite the fact that there are multiple current alternatives, there is nevertheless potential for progress because of the earlier-mentioned restrictions.

(3) Blackhole attack: Despite the presence of various known vulnerabilities methods for blackhole attacks, many of them come with serious problems, including presuming the existence of only one rogue node, and that in practical situations is unachievable, or becoming computationally or resource intensive. To address the problem, additional encryption techniques to prevent blackhole attacks should be created.

(4) Grayhole attack: The grayhole attack is considered one of the most common assaults on in-vehicle systems and therefore is challenging to recognize owing to the rogue node's duplicitous structure. Appropriate security alternatives have a few more disadvantages, such as the fact that several recommended methodologies hardly understand arithmetical quantities as information and that few rely on traditional networks procedures, causing a reduction in effectiveness; consequently, special security alternatives may indeed be constructed by having to consider encryption algorithms for protecting against grayhole breaches in a system.

(5) Wormhole attack: Another of the most prominent assaults in IoV is the wormhole threat. For the wormhole attack, the researchers have discovered since appropriate security measures to avoid such assaults include a few shortcomings, including significant energy usage due to the enormous number of terminals, and the outcomes of these approaches are really not comparable to others. Since these inadequacies, limited enhanced security technologies to defend systems against wormhole attacks may be created in the future.

(6) Sinkhole attacks: Sinkhole attacks constitute one of the most common in-vehicle networking assaults. Several safety solutions have been designed by various studies, but all possess restrictions, like the failure to recognize suspicious sinkhole gateways in the environment of multiple threats or when they occur close to access points. To prevent systems from certain assaults, enhancements to present cryptographic techniques are necessary.

(7) Node impersonation attack: This attack is also well-known however the creators failed to put in much effort to build security mechanisms for that though. The options provided were ineffective at safeguarding the infrastructure as well as entail significant complexity but also latency. As a response, this assault should be taken into account, and adequate protective measures should be proposed.

(8) Man-in-the-middle one: The man-in-the-middle is a common assault in IoV. Such assault received little attention from academics. Furthermore, a computation for the suggested technique necessitates a long time. As a result, enhanced security measures must be taken to safeguard the system against this assault.

### A. GPS Spoofing Attacks

Spoofing attacks on GPS (Global Positioning System) too are common in automotive networks. To put a halt to this assault, equally efficient and safe alternatives must be developed.

(1) Masquerading assault: A further difficult technique in IoV is the masquerading attack. There are relatively few protection options available for such an attack. As a consequence, counterintelligence for this assault is required to protect the infrastructure against impersonating assaults.

(2) Trust: Trust is an essential component of communicating devices, particularly whenever entities deal with outsiders. For instance, whether certain could a base station be that yet another cluster will share its information with them. Of being sustainable, every cryptographic signature must include a distinctive, permanent, as well as differentiated identity. If nodes possess non-persistent (with a limited lifespan) identity, they may alter identity for subsequent interactions, however, non-distinct identification also had no one-to-one matching among identities as well as cars that seems to be, upwards of single identification on such a single car: Sybil attack. Inside the framework of the legislation, one would wonder whether trust-related data could be maintained and handled on a huge scale. Alternatively, more particularly, how might trust data be used safely. Identity guarantee should indeed be provided via forthcoming authentication mechanisms. Devices on such a system could indeed develop trust except if the trust system developers handle this identification initially. Interaction activities are very vital in establishing trust in the system. The algorithms should be flexible as well as suitable for being dispersed. Furthermore, it must guarantee appropriate mappings of intuitive to quantitative trust and be computationally effective.

(3) Resilience and Self-Adaptation: An important area to explore is the shift between lowering vulnerability to boosting resiliency and self-adaptation. The IoV platform must be robust enough to respond fast and comprehensively against assaults and odd behaviors. For reliability, experts in the IoV area must examine and apply AI-based solutions such as automated software patching and self-rewriting code.

(4) Privacy protection: The great majority of IoV apps make use of internet services. Third-party cloud-based applications could not always be a reliable solution for outsourced processes. Cloud-based solutions are used by the great majority of IoV software. As a result, entrusting outsourced duties to third-party providers of cloud-based services does not always ideal. It would be even more enticing to use cloud-based services that may not require the information compiled. Techniques for maintaining confidentiality in data storage operations that are now in use employ partly and entirely efficient encryption standard techniques. Nevertheless, such methods need a substantial amount of resources, especially while computing a large amount of information generated by multiple automobiles in the IoV scenario. To secure users as well as privacy protection in the IoV environment, lightweight fully homomorphic encryption is required. On the cloud platforms, for instance, customers' identities should be needed for authorization but they cannot be anonymous credentials. Protecting responsibility and confidentiality while simultaneously preserving anonymity is what regulated anonymity entails. Individuals, for instance, may not be so unidentified as to undermine responsibility, but they must also not even be unknown to jeopardize confidentiality.

(5) AI-based detection: There is currently a global lack of security personnel. The usage of robots and self-driving cars will grow in the future. It will be important to develop an AI-based immune system capable of dealing with unexpected dangers dynamically, protecting from potential vulnerabilities including abnormalities, while responding to AI-based ransomware, cognitive hackers, and others. Chrysler recalled nearly 1.4 million vehicles as

a consequence of the breach. The Chrysler Jeep Cherokee did not represent the only automobile shown to be susceptible to intentional tampering.

### B. The communication layer

The communications layer primarily consists of communication between vehicles which might happen both within and outside an automobile. Interior vehicle communication may occur inside the in-vehicle Networking, sometimes referred to as the automobile networking or intra-vehicle communications system. The interconnectivity of the various Electronic Control Units (ECUs) inside a car's technological components is the foundation of in-vehicle networking.

External vehicle communication is done when automobiles link directly to USBs and maintenance equipment, distantly to Remote Keyless Entry systems, or participate in Channel access that allows messages to be exchanged among infrastructure and cars. To ease V2X communications, linked and self-driving cars may act as stations in self-organized vehicular ad-hoc networks (VANETs). VANETs have been mainly made up of two kinds of mobile nodes: On-Board Units (OBUs) and Road-Side Units (RSUs). OBUs include wireless communicators that are placed in V2X-enabled automobiles. Cars equipped with OBUs may interact with each other in addition to Road-Side Units (RSUs), which seem to be static equipment situated alongside roadways and other infrastructure which can offer internet service for OBUs and monitor traffic situations.

### C. OBU and RSU

Security problems in the vehicle connectivity result in four automotive security problems, as follows: Restricted connection: While automotive exterior communication is improving, many cars still lack the capacity to upgrade their programming from OTA updates that would also allow automobiles to constantly be secured against the newest computer hackers.

Although if OTA upgrades grow more common, cars may remain vulnerable to failures caused by inadequate upgrades. Computational performance is limited: In principle, vehicle computing capacity is restricted when contrasted with desktop computing capabilities. Since automobiles get a longer life expectancy and should withstand greater heat and shocks than usual computers or laptops, that constraint occurs. Automobiles are far more prone to still be attacked than desktops due to their processing deficit. Due to automobiles' restricted processing capability, several automotive security technologies will require too big operating costs to be applied.

Risks and assault situations that are unexpected: Numerous various access routes may be used to penetrate a vehicle infrastructure, namely vehicle database, distant communications technology, and automotive components. New threats were constantly being made, making it challenging for manufacturers to forecast wherever cybercriminals will target next. Unsecured Original Equipment Manufacturers (OEM) products may give attackers many extra network nodes in an automobile.

Significant risk to the safety of driver or passenger: Regardless of whether only a few detectors are misled or a limited handful of illicit signals are received, an automobile may have faults that jeopardize the safety of motorists, travelers, and bystanders.

The three-layer Autonomous Vehicular Sensing Communication Control (AutoVSCC) architecture may help understand risks to communication between vehicles. The perception layer is located at the bottom of the hierarchy and therefore is subject to spoof as well as eavesdrop assaults on different sensors including inertial or radio detectors. The data communication is situated above the perception layer and includes both inter-vehicular as well as intra-vehicular interactions. It is sensitive to eavesdrop assaults as well as information manipulations among cars as well as roadside units. Risks that transmit upstream from the perception layer, which again is composed of different sensors, are equally vulnerable to the communication layer. Risks at both the sensor and communication levels might have an impact on the upper tier, the control layer, that covers autonomous vehicle control activities including speed limit and braking system.

Furthermore, an introduction of such a three-layered structure (perception, communications, and controlling) of self-driving and connected automobiles is offered, followed by a discussion of several levels that seem to be susceptible to cyberattacks. Moreover, this study provides a comprehensive evaluation of the dangers to vehicular networks based on existing research information. The topic of intravehicular safety is covered, with either an emphasis on automobile public transport systems, entertainment and telemetry structures, and automotive terminals. Furthermore, V2X safety is explored concerning distant technologies, clusters, databases, vehicle-to-vehicle connectivity, and vehicle-to-infrastructure interaction. Then, viable responses to different dangers in V2X communications were described in depth.

## ░3. THREATS IN VEHICULAR NETWORKS

Network Access assaults, Transport Confidentially assaults, Traffic Integrity threats, and Denial of Service attacks are all serious targets of Ethernet communications [15-21].

### A. Network access assaults

Intruders may get entrance to the Ethernet connection via internet connectivity operations. Such assaults might well be carried out independently or in combination with other kinds of assaults, such as seizing control of those other servers or routers. Intruders may technically enter an Ethernet connection by attaching to an unsecured socket on a switch, or they could employ malicious code to get remote control of the network.

### B. Traffic confidentiality attacks

Whenever hackers have acquired access to the system, attackers may use traffic confidentiality assaults to eavesdrop on data transmission. Hackers may deliver texts but also examine their responses to learn about the network component as well as architecture. Hackers could eavesdrop together on internet activity by attaching tracking devices to cabling linking a server and then a router between these devices. When switches are confused about where or how to send a message, it will be flooding the block to all endpoints. Intruders may use this functionality to launch MAC flooding assaults. They may listen across all packets during such assaults by rewriting a MAC table, causing all network packets to be inundated.

### C. Traffic integrity attacks

Two methods used during Ethernet communications seem to be the Address Resolution Protocol (ARP) as well as the Dynamic Host Configuration Protocol (DHCP). Intruders may broadcast ARP responses to collect network activity and react to DHCP server queries to influence internet traffic throughout ARP and DHCP poisoning assaults. Such assaults may be antecedents of man-in-the-middle assaults, whereby reroute networking communication to an assailant's nodes in order to modify data. Session hijacking and replay attacks are two further forms of traffic integrity threats. Throughout a Session hijacking attempt, hackers may eavesdrop to find session results generated by protocol implemented across Ethernet, subsequently posing to be one of the event's endpoints or interfering with the event.

### D. Denial of Service (DoS) attacks

Denial of service (DoS) assaults disrupt internet accessibility by breaking physical hardware or overloading the network. Layer 1 assaults actually destroy connections or equipment, rendering the internet connection useless. Layer 2 assaults may be resource exhaustion assaults, that are using network bandwidth by transmitting packets to be decoded incessantly, or protocol-based denial of service attacks, that employ the self-configurable Spanning Tree Protocol (STP) to transmit STP signals incessantly.

## 4. APPLICATIONS DEVELOPED FOR V2V COMMUNICATION SYSTEMS

Mobile improvisational networking serves as the foundation for software built for inter-vehicle communication devices. These communication networks are essentially being converted to cars and are being given the term VANET (Vehicular Ad-Hoc Networks) (Figure 3). Components interact among themselves inside this arrangement. Components on cars are referred to as OBU (On Board Unit), components in infrastructures or highway elements are referred to as RSU (Road Side Unit), whereas components on the central servers are referred to as SU (Server Unit) [22-26]. Every module interacts with the other modules through a set certificate as well as hierarchical rules. If the certificate hierarchies, description, and time need not alter in the manner they would prefer to apply it, it results in distinct procedures and applications. As a result, the applications detailed within the following part are essentially similar, notwithstanding differences in certifications and connection requirements.

### 4.1. SeVeCom

The SeVeCom initiative is a partnership between many EU-sponsored automotive manufacturers, supply firms, institutions, as well as the government. As previously stated, the project was designed using the VANET basic architecture. In contrast to the underlying principle, the EU had adjusted the certification administration to lower network activity at the point of intersection, as they desired. Essentially, ELP (Electronic License Plate) distribution through RSUs is being investigated again for certifying technique, but PKI (Public Key Infrastructure) was already chosen because this operation may be performed or duplicated.

PKIs that have been established are constantly disseminated between basic computers. The OBU and the RSU communicate, and data is sent to the basic computers through the RSU. The network is rendered available by preventing needless certifying loads from being overburdened by this design.

### 4.2. GeoNetworking

The concept does not really contain RSUs or servers in VANET networks. Every unit inside a 100m radius is linked together by employing the same IPv6 standard as the wireless network technologies used throughout modern PCs.

Instead of offering a global information exchange, the major goal is to link the tools to manage congestion in a specific region. Existing computer systems include vulnerabilities due to the usage of the IPv6 protocol.

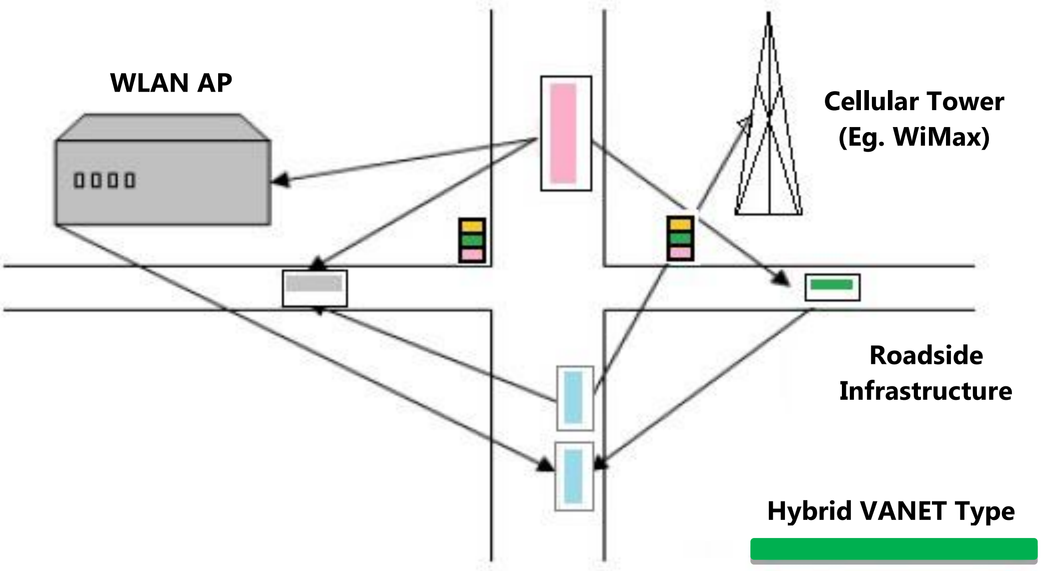

**Figure 3.** An example of VANET architecture

### 4.3. Intersafe

The groundbreaking initiative Intersafe in Europe is seeking to produce a simple Intersection Assistant. The initial effort by this assistance to decrease accidents and deaths is to ensure that the vehicle is informed of the automobiles surrounding it. It intends to achieve this goal through the use of thousands of sensors and two-way communication technologies utilizing IEEE 802.11. Upon this basis, multiple incidents may be predicted and many other motorists could be informed. The second option is to handle traffic signals. Traffic signals with detectors and bi-directional radio transmission depending on IEEE 802.11 may indeed offer the necessary precautions by notifying oncoming cars more about traffic signal state, driving conditions, and possible incidents.

### 4.4. Universal Traffic Management Society of Japan (UTMS)

UTMS (International Traffic Management Society - Japan) is developing an information technology infrastructure that will respond to every one of the situations stated previously. On the roadway, IR and limited communication indicators are employed throughout this technique. The above sporadically broadcast indicator enables the automobile to exercise caution in the motor by transferring static texts including location and traffic regulations, in addition to the car's location on that road, in addition to varying texts including other automobiles as well as human locations but also speeds. The attached device does a vulnerability assessment and undertakes safeguards by informing the motorist in the event of a threat.

### 4.5. Cooperative Intersection Collision Avoidance System (CICAS)

The CICAS (Cooperative Intersection Prevention Systems Initiative) offers real alerts to cars and infrastructural employees. The system is constructed of many components that employ traffic information, roadside accessories, junction mapping, and two-way transceivers. The preliminary of them is a traffic signal violation alert system. The technology not only notifies drivers regarding traffic signals, and moreover runs traffic speed and positions via a risk assessment, recognizing automobiles that do not violate traffic signals and notifying nearby automobiles, including converting all lights in the circle to red. A similar feature is the stop light helper that alerts the motorist about the impending halt sign. Likewise, another system will alert cars that would drive left to those other automobiles and arcs and performs the most accurate maneuvering evaluation.

## 5. ARCHITECTURE AND COMPONENTS OF IN-VEHICULAR SYSTEM

In-vehicle networks (IVNs) are indeed a new study topic within vehicular communications. The in-vehicle communication system is made up of multiple fundamental elements, including the Sensor Domain, which includes highly precise detectors, the Chassis Area, the Infotainment Area, the Telematics Area, and the Powertrain Area, among others. Standards like Ethernet, FlexRay, and Controller Area Network (CAN), among others, play a significant role in ensuring the communication process between any of these necessary elements of in-vehicle networking. The fast expansion of connection between transportation systems integrated with modern advanced devices, such as V2Xcommunications, has contributed to the broadening of known vulnerabilities, allowing attackers to gain entry to the in-vehicle networking.

### 5.1. Internal Arrangement of Electronic Control Units

Important data is transmitted between the car's various electronic control units (ECUs). Because as the quantity of ECUs in sophisticated contemporary automobiles rises, thus does the consideration of many factors in in-vehicle networking, because every individual part has available frequency as well as delay needs. This same quantity of ECUs in current intelligent cars is constantly increasing in order to provide the advanced technological automobile with a variety of innovative functions for protection, reliability, efficiency, and more.

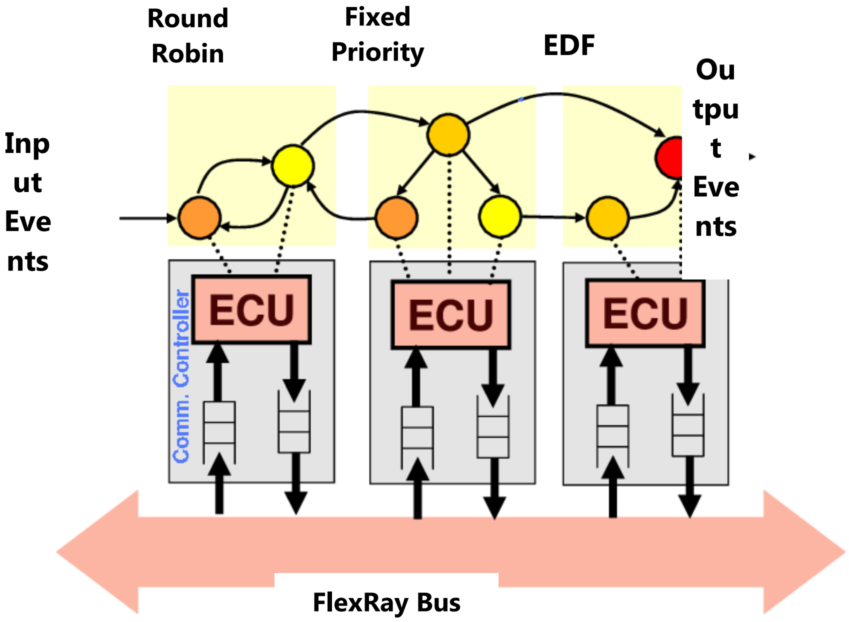

**Figure 4.** Network Configurations of ECUs

Furthermore, numerous in-vehicle standards have already been created enabling the interconnectivity of a significant number of ECUs, while development into far more advanced capabilities is ongoing. Furthermore, because of the diverse functions, such as automotive assessment and management, ECUs are often linked to much more than just the bus network. Figure 4 depicts in depth the internal network setup of ECUs.

### 5.2. In-Vehicle Network Infrastructure

In-vehicle networks sometimes referred to as internal communications infrastructure, are already in charge of linking multiple parts inside contemporary sophisticated automobiles. ECUs, interfaces, detectors, controllers, and others are regarded the essential fundamental characteristics within contemporary intelligent cars. Furthermore, the technique provides a car containing many components, such as Telematics Area, Infotainment Area, Chassis Area, Powertrain Area, Body Area, and Sensor Area, among others. Sensors provide data to such electrical components for some further processing.

### 5.3. Classification of In-Vehicle Network Architecture

There are three kinds of in-vehicle system architecture. The first categorization encompasses the central gate, which is characterized as the decentralized electrical and electronics (E/E) type of design. The domain-centralized electricals and electronics (E/E) design connect multiple functional areas through a single gateway in the next categorization. Future E/E architecture also referred to as zonal infrastructure, is the third aspect of in-vehicle system architecture. This design includes a centralized high-performance computing unit (HPCU), that helps to reduce the complexities of the preceding two systems.

The platform's two foundational pillars are function-specific ECUs and a central gateway. For connecting, the controller area network (CAN) connection is employed. Also with the support of the central gateway, ECUs could work together effectively. As a result, with the aid of a centralized gateway, complicated operations including cross-functional connectivity and adaptive cruise control may be implemented quickly in this sort of infrastructure.

Because multiple ECUs interact through a common gateway, the fundamental drawback of electrical and electronics (E/E) type in-vehicle network design is higher communications latency. To solve this issue, a framework for in-vehicle network technology depending on various roles and functions was created, wherein distinct functional/operational areas are coupled through the central gateway. Furthermore, because the majority of communication occurs inside these operational and functional domains, the connection burden on the central gateway is greatly decreased. This design is flexible since more functional areas may be readily incorporated.

### 5.4. CAN-Centric Safety Risks

Bus-off attacks, denial of service (DoS), masquerade, injecting, spying, and replay attacks were all mentioned in scientific journals on CAN bus systems. Because CAN messages are often not secured and therefore do not enable authentication services, hackers could get information about the CAN packet, therefore, gain easy access to the system; this sort of assault is characterized as a Masquerading assault. Furthermore, the transmitted vehicular CAN communications could well be spied on by hackers, allowing them to enter into the in-vehicle networks; this would be characterized as an overhear assault. The hackers could then attempt to send fake messages over the car's bus network. Using OBD-II connections, hackers could effectively access the in-vehicle network and thus, as a result, attempt to hack the ECUs; this form of assault is characterized as an injection attack. Furthermore, the hacker could impede the car's real-time functioning by repeatedly re-sending genuine data; this form of assault is termed a replay attack. Additionally, the hacker could transmit bytes in the identity column and some other fields continuously. This would be referred to as a bus-off assault. Furthermore, the hacker could interrupt the regular execution of in-vehicle connectivity by continually providing high-priority CAN packets that block legal low-priority messages and might even seize the controls of the vehicle; this form of assault is characterized as a DoS attack. The very first basic rule for preventing such threats would be to utilize encryption and verification of communications transmitted between two ECUs.

## ░6. LITERATURE REVIEW

This section gives a brief literature review of the existing vehicular security mechanisms [27-36]. VANET and IoV security and confidentiality concerns In this section, we will look just at concerns about security and privacy that exist including both VANETs and IoV. Since the IoV emerged through VANETs, the assault range could have a higher correlation. Nevertheless, we will address each of the following subdomains individually. Automobiles in VANETs may transmit helpful information about numerous major events, including road surfaces, traffic jams, and disaster warnings, to enable effective as well as dispersed transport infrastructure. Automobiles may receive this type of data from other automobiles or the surroundings to spot traffic jams or crashes.

During such a crucial circumstance, any existence of hostile as well as uncooperative routers producing faked or manufactured information diffusion in the system might result in disastrous events, jeopardizing prospective users' safety, privacy, and confidentiality. Since VANETs originated through MANETs, the dangers offered by VANETs are mostly retained from ad-hoc design of MANETs that are often targeted from a narrow spectrum since cars are rarely associated with the Internet. Intervehicle and intra-vehicle assaults upon VANETs are the most common inter-vehicle combat.

Due to the absence of centralized management and supervision in VANETs, security mechanisms requiring centralized trustworthy third party (TTP) or all-time connection, including public key infrastructure (PKI), could not be deployed, thereby opening the door to major assaults at several stages. Furthermore, the absence of a comprehensive system for managing identities renders VANETs an appropriate target for identification assaults like Sybil. A Sybil hacker may construct or maintain several bogus identities in the networks that communicate incorrect facts to create a mistaken impression of non-existent occurrences. For instance, disseminating wrong information created by Sybil hackers regarding fictitious highway congestion problems and disasters may be used to intentionally divert traffic for theft, abduction, or automobile stealthy objectives, that are harmful to motorists' and/or automobiles' security and protection. Likewise, a hacker may acquire the passwords of unsuspecting nodes with the goal to abuse the privileges and entitlements connected with some of those credentials or to install malicious or unruly behaviors (including denial of service (DoS) assaults) inside the networks without first being held responsible for these kinds of activities. This is known as an impersonating or masquerading assault.

VANETs are indeed subject to packet error attacks, including black holes, grey holes, and wormhole assaults, which might also cause DoS attacks on one or a group of vehicles. Automobiles are linked to certain other members of the network by wireless connectivity channels, rendering them subject to numerous types of threats including traffic monitoring, jam, as well as spying. These are a few of the VANET-related assaults. Contemporary automobiles now feature an assortment of sensors that are involved in a wide range of activities, including assessing inter-vehicle separation as well as road surfaces, detecting fires and smoke detecting automobile acceleration/deceleration, detecting obstacles, and so much more. Intra-vehicle assaults are dangerous to the car driver as well as the car's security and stability, since deceiving a detector could injure the automobile and/or the operator. An assailant, for example, may threaten the victim's life by disconnecting the brake system as well as the wheel in a driverless vehicle. On the contrary side, because of the combination of different systems, protocols, and applications in IoV, there is going to be a strong degree of diversity; as a result, the need for privacy and confidentiality would rise. Linking cars to the outside environment could offer significant risks and subject the IoV to a broader assault range than that of the VANET. There seem to be different security flaws in IoV as a consequence of unsecured operations in V2I and V2C contexts.

Automobiles are associated with the Internet, making them accessible to personal attackers and evil groups all across the world. It leaves both cars as well as the internet vulnerable to cyber criminals or hackers. By attacking insecure interconnections or altering numerous vehicle streams of data, malicious hackers might have disastrous consequences. MP3 format, for example, may swiftly corrupt the entire system of automobiles.

Whenever unauthorized individuals gain access to the car's information system through software or even other methods, hackers may influence numerous automotive components including the steering wheel, warning system, and braking system. This had been proved effectively at a previous Black Hat cybersecurity conference. The IoV's reliance on cloud computing gives up an additional avenue for computer hackers since cloud services are indeed potential destinations. For instance, malicious hackers could utilize malware to generate cash through cloud-based service providers, or they might simply launch DoS or distributed DoS (DDoS) assaults on the infrastructure to disturb prospective consumers. If robotic attackers using artificial intelligence (AI) or big data analytics were utilized against certain internet services, the issue would worsen.

Previously, the Defense Evolved Research Projects Agency (DARPA) held an all-machine hacker event, indicating that should the subject advance, robotic attackers might pose a significant threat to cyber defenses. Additionally, it has been proven that robots, including botnets of machine attackers, could find software faults as well as flaws quicker than people and may execute higher devastating or destructive cyber-attacks than individuals.

## ░7. CELLULAR V2X (C-V2X)

Vehicle-to-everything connectivity may make advantage of distant communications technology. Information may be sent among onboard or roadside equipment by using means of communication. Weak points in distant communications technologies may be targeted by hackers for the goal of messing severely only with the operation of a vehicle or buses out of a respectable distance. As a result, hackers are no longer required to attach peripherals to car terminals in order to get access to automotive network communication designs. Wireless transmission solutions have various drawbacks, which hackers might exploit. It divides distant communication systems into numerous areas, including keyless entry systems (RKE), wireless access in-vehicle systems, Zigbee, radio frequency identification (RFID), WiMAX, and Wi-Fi.

Cellular V2X (C-V2X) was created by 3GPP1. The above technique has two modes of operation. The first form is device-to-device, that comprises vehicle-to-vehicle (V2V), vehicle-to-pedestrian (V2P), and vehicle-to-roadway infrastructure (V2I). Given that there is clear relation inside this form, connectivity does not need synchronization. The second way is device-to-network (D2N) or vehicle-to-network (V2N). This method provides a variety of cloud services through wireless connections.

### A. Associated Threats

Several changes have been made to the security mechanisms of LTE and LTE-Advanced networks. Researchers gave a description of the security mechanisms of the LTE and LTE-Advanced networks, in addition to an investigation of the security vulnerabilities in the LTE and LTE-Advanced network design. LTE networks are susceptible to insertion, manipulation, and surveillance assaults, among other security concerns. As a result, it poses greater privacy implications than GSM and UMTS. An innovative security assault targeting variations of the authentication and key management (AKA) standard, assault violates users' confidentiality more thoroughly than conventional assaults. Researchers demonstrate how knowing SQN minimally contributes to remote monitoring assaults. The LTE network is vulnerable to different assaults including IP spoofing, DoS attacks, malware, ransomware, and so on. Since the debut of the LTE femtocell, the hacker has obtained HeNBs (Home enodeB). The hackers may change the functioning of the unit to suit their needs. There seem to be two kinds of security mechanisms: (a) Data encryption of user information, and (b) The platform's authorization. A methodology for assessing various LTE routers was created.

## 8. CONCLUSION

To avoid road accidents, it is initially required to understand where incidents occur most frequently. Accidents have happened most frequently near traffic crossroads, according to studies conducted in numerous nations. The most common situations which create collisions on the interstate include failure to respect the traffic signal, failure to observe the red light, negligence in paying respect to other cars in turning, collisions with the pedestrian, sudden braking rear contact, and unregulated junction. Furthermore, since road traffic is disturbed after some accidents, cars that are not aware of the collision cause a new collision. This study expands on considerations about cybersecurity problems regarding cybersecurity challenges and mitigation strategies in intelligent transport systems as well as vehicle communications.

**Declarations**

***Source of Funding***

*This research did not receive any grant from funding agencies in the public, commercial, or not-for-profit sectors.*

***Competing Interests Statement***

*The author declares no competing financial, professional, or personal interests.*

***Consent for publication***

*The author declares that he/she consented to the publication of this research work.*

**References**

[1] A. Serageldin, H. Alturkostani, and A. Krings (2013). On the reliability of DSRC safety applications: a case of jamming. International Conference on Connected Vehicles and Expo, Pages 501–506.

[2] B.K. Chaurasia, R.S. Tomar, S. Verma, G.S. Tomar (2012). Suitability of manet routing protocols for vehicular ad hoc networks. In 2012 International Conference on Communication Systems and Network Technologies, IEEE, Pages 334–338.

[3] C. Laurendeau and M. Barbeau (2006). Threats to security in DSRC/WAVE. In Proc. 5th International Conference on Ad-Hoc Networks & Wireless, LNCS 4104, Pages 266–279.

[4] Adebowale A, Idowu S, Amarachi AA. (2013). Comparative study of selected data mining algorithms used for intrusion detection. International Journal of Soft Computing and Engineering, 3(3): 237–241.

[5] N. A. Khan, A. M. U. Siddiqi, and M. Ahmad (2021). Development of Intelligent Alumni Management System for Universities. Asian Journal of Basic Science & Research, 3(2): 51–60. doi: 10.38177/ajbsr.2021.3206.

[6] H. Hasbullah, I. Soomro, and J. Ab Manan (2010). Denial of service (DOS) attack and its possible solutions in VANET. International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering, 4(5): 813–817.

[7] Anil Lamba (2013). Enhancing Awareness of Cyber-Security and Cloud Computing using Principles of Game Theory. International Journal of Advanced in Management, Technology and Engineering Sciences, III(I): 71–82.

[8] J. Härri, F. Filali, C. Bonnet, M. Fiore (2006). Vanetmobisim: generating realistic mo-bility patterns for vanets. In Proceedings of the 3rd International Workshop on Vehicular Ad Hoc Networks, ACM, Pages 96–97.

[9] J. Harri, M. Fiore (2006). Vanetmobisim–vehicular ad hoc network mobility exten-sion to the canumobisim framework. Institut Eurécom Department of Mobile Commu., 6904: 1–19.

[10] Lamba, A. (2014). Cyber Attack Prevention Using VAPT Tools (Vulnerability Assessment & Penetration Testing). Cikitusi Journal for Multidisciplinary Research, 1(2).

[11] S. Alangari and N. Ahmed Khan (2021). Artificially Intelligent Warehouse Management System. Asian Journal of Basic Science & Research, 3(3): 16–24. doi: 10.38177/ajbsr.2021.3302.

[12] L. Bononi, M. Di Felice, M. Bertini, E. Croci (2006). Parallel and distributed simulation of wireless vehicular ad hoc networks. In Proceedings of the 9th ACM In-ternational Symposium on Modeling Analysis and Simulation of Wireless and Mobile Systems, ACM, Pages 28–35.

[13] M. Brooker (2007). Mutual interference of millimeter-wave radar systems. IEEE Transactions on Electromagnetic Compatibility, 49: 170–181.

[14] M. Piorkowski, M. Raya, A.L. Lugo, P. Papadimitratos, M. Grossglauser, J.-P. Hubaux (2008). TRANS: realistic joint traffic and network simulator for vanets. Mob. Comput. Commun. Rev., 12: 31–33.

[15] N. Li and Y. Zhang (1995). A survey of radar ECM and ECCM," IEEE Trans. Aerospace and Electronic Systems, 31(3): 1110–1120.

[16] N. Wisitpongphan, O.K. Tonguz, J.S. Parikh, P. Mudalige, F. Bai, V. Sadekar (2007). Broadcast storm mitigation techniques in vehicular ad hoc networks. IEEE Wirel. Commun., 14: 84–94.

[17] Anil Lamba (2014). Uses of cluster computing techniques to perform big data analytics for smart grid automation system. International Journal for Technological Research in Engineering, 1(7): 5804–5808.

[18] Q. Xu, T. Mak, J. Ko, and R. Sengupta (2004). Vehicle-to-vehicle safety messaging in DSRC. In Proceedings of the 1st ACM International Workshop on Vehicular ad hoc Networks, Pages 19–28.

[19] S. Farné, F. Benzi, and E. Bassi (2020). IIoT Based Efficiency Optimization in Logistics Applications. Asian Journal of Basic Science & Research, 2(4): 59–73. doi: 10.38177/ajbsr.2020.2406.

[20] J.Rani & G.Glorinda (2021). A Simplified Fractal Texture Analysis Approach using Quadtree Decomposition with Huffman Coding Technique. Middle East Journal of Applied Science & Technology, 4(3): 01–09. doi: 10.46431/mejast.2021.4301.

[21] Anil Lamba (2015). To classify cyber-security threats in automotive doming using different assesment methodologies. International Journal for Technological Research in Engineering, 3(3): 5831–5836.

[22] K. Pawar, C. Ambhika, and C. Murukesh (2021). IoT Hacking: Cyber Security Point of View. Asian Journal of Basic Science & Research, 3(2): 01–09. doi: 10.38177/ajbsr.2021.3201.

[23] S. Bohacek, V. Sridhara, J. Kim (2000). Udel Models for Simulating Urban Wireless Networks.

[24] Anil Lamba (2016). S4: A novel & secure method for enforcing privacy in cloud data warehouses. International Journal for Technological Research in Engineering, 3(8): 5707–5710.

[25] Debar, M. Dacier, and A. Wespi (2000). A revised taxonomy for intrusion-detection systems. In Annales des télécommunications, 55(7–8): 361–378.

[26] S. Roome (1990). Digital radio frequency memory. Electronics & Comm. Engineering Journal, 2(4): 147–153.

[27] S.-Y. Wang, C.-L. Chou (2009). Nctuns Simulator for Wireless Vehicular Ad Hoc Net-work Research. Ad Hoc Networks: New Research, Nova Science Publishers.

[28] Anil Lamba (2017). Analyzing and fixing cyber security threats for supply chain management. International Journal for Technological Research in Engineering, 4(5): 5678–5681.

[29] D. M. Farid, N. Harbi, and M. Z. Rahman (2010). Combining naive bayes and decision tree for adaptive intrusion detection. Arxiv preprint arXiv:1005.4496.

[30] M. Goldstein (2012). FastLOF: an expectation-maximization based local outlier detection algorithm. In 21st international conference on Pattern recognition (ICPR), Pages 2282–2285.

[31] Hall M, Frank E, Holmes G, Pfahringer B, Reutemann P, Witten IH. (2009). The WEKA data mining software: an update. ACM SIGKDD explorations newsletter, 11(1): 10–18.

[32] V.Richard (1976). Millimeter wave radar applications to weapons systems.USA Ballistic Research Lab.

[33] V.D. Khairnar, S. Pradhan (2013). Comparative study of simulation for vehicular ad-hoc network. Preprint, ArXiv: 1304.5181.

[34] W. Zhang, H, Zeng, Y, Li, and X. Wang (2009). Polarimetric radar performance test of signal processing for anti-active jamming. IET International Radar Conference, Pages 1–4.

[35] X. Qiao, T. Jin, X. Qi, M. Zhang, S. Yuan, and Q. Zhang (2007). Anti-millimeter wave polarization agile active jamming. In Proceedings of the International Conference on Microwave and Millimeter Wave Technology, Pages 1–4.

[36] Y.P. Fallah, C. Huang, R. Sengupta, H. Krishnan (2010). Congestion control based on channel occupancy in vehicular broadcast networks. In 2010 IEEE 72nd Vehicular Technology Conference-Fall, IEEE, Pages 1–5.