JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Securing Automotive Sensor Systems: Mitigating Cybersecurity Threats

[1]Yokeshwar M, [2]Prof.Yashaswini B M

[1]Student, [2]Assistant Professor
[1,2]Department of Computer Science and Information Technology,
[1,2]NJain (Deemed-to-be-University), Bangalore, India

Abstract: in today's automotive scene, automobiles are outfitted with a plethora of sensors ranging from sixty to one hundred, which exemplify the features of Cyber-Physical Systems (CPS). The interaction of the many components inside the vehicle's CPS, including sensors, devices, and systems, demonstrates a high degree of coupling and cohesion across the sensing, communication, and control levels. Notably, the interdependence is vulnerable to cyber threats, since assaults on the sensing or communication levels might jeopardise the security of the control layer. This paper delves deeply into the possible cyber dangers connected with contemporary automobiles' sensor layers. The primary focus is on two types of sensors: vehicle dynamics sensors (such as TPMS, magnetic encoders, and inertial sensors) and environment sensors (such as LiDAR, ultrasonic sensors, cameras and GPS units). Furthermore, the paper examines existing countermeasures offered in the literature.

***Keywords* - cyberattacks, vulnerable sensors, sensing layer, vehicle dynamics sensors.**

I. Introduction

We are entering an era in which partially and completely autonomous vehicles are about to become a reality on Indian roadways. The National Highway Traffic Safety Administration vehicles by 2025. Meanwhile, the NHTSA encourages Indian auto and technology firms to create partially automated technologies such as lane-keeping aid, adaptive cruise control, and self-parking. Manufacturers such as Tata Motors, Mahindra Electric, and other Indian automotive industry companies are already using vehicular sensors to allow completely autonomous and semi-autonomous functionalities, which are being actively tested on Indian roads. The Society of Indian Automotive Engineers conducted a poll to identify cybersecurity vulnerabilities associated with autonomous cars in India. Ensuring the safe deployment of SAE Level 5 autonomous cars in India necessitates a thorough examination of cybersecurity issues during the decision-making process [1]. Autonomous cars in India use sophisticated sensors to assess their surroundings, monitor road conditions, recognize Indian traffic signs, detect collisions, and estimate distances. While Indian human drivers frequently make right judgements despite poor senses, the existing decision-making algorithms in autonomous vehicles are still developing. This gives hostile actors the ability to compromise vehicular sensors and perhaps cause disruptions on Indian highways [2].

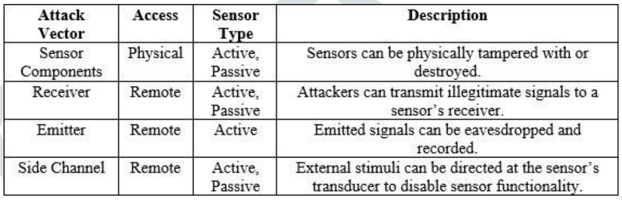
Instances of different attack types on unmanned aircraft systems and robotic locomotives have been documented worldwide, however data on autonomous vehicle sensor assaults in India is restricted due to quick solutions by Indian vehicle makers. India- based researchers have also found cybersecurity dangers in sophisticated driver assistance technologies, such as camera system attacks and object detection algorithm manipulation. Vehicular sensors are not the only vulnerability in India; attackers might exploit connected and autonomous cars by attacking roadside infrastructure or compromising the security of ride-hailing customer data stored in the cloud. While Over-The-Air (OTA) updates provide remote software repairs, there is a danger of security vulnerabilities. Physically Unlosable Functions (PUFs) are becoming increasingly important for safe OTA decryption in India. Securing the Indian automotive supply chain and creating cybersecurity guidelines for third-party manufacturers are also critical to preventing car component failures. Despite vehicle protocol regulations prohibiting updates while the vehicle is in motion, experiments reveal weaknesses in Electronic Control Unit (ECU) re-flashing, underscoring the necessity for OTA updates in the Indian automotive sector [3].

II. Literature Review

A. Automotive Systems and Sensing Layer Integration Overview

Automotive security hazards are classified using a three-tier hierarchical method called the Auto VSCC architecture. The layer that detects is made up of vehicular sensors, which are the framework's core stratum. Possible dangers to this layer include GPS jamming, eavesdropping on communications inside Tyre Pressure Monitoring Systems (TPMSs), and tricking ultrasonic sensors into reporting phantom objects [3]. Risks originating in the sensing layer can spread to the communication layer via the physical- datalink interface. This interface converts analogue sensor input into digital data, which is critical for both among and intra- vehicle interactions. The vulnerabilities in the interactions include transmitting incorrect signals (via its communication buses). Threats to the sensing and communication layers might have a knock-on effect on the control layer's functioning. This influence is seen through the transport-application interface [4]. The vehicular sensing layer comprises of 60 to 100 sensors that measure a vehicle's status and surroundings, which are critical for electronic control systems making driving choices. For example, distance sensors allow adaptive cruise control to determine safe speed increases. In autonomous cars, vehicular sensing substitutes human sense, necessitating excellent dependability. As automation advances, automakers may raise the number of sensors to about 200, with each providing a specialized function like safety, diagnostics, convenience, and environmental monitoring. Safety sensors include night vision, impact detection, and personalized airbag deployment. Diagnostic sensors detect faults and notify drivers. Convenience sensors monitor air quality, regulate mirrors, enable automated braking, adjust wipers, and detect rain and fog. Environment monitoring sensors monitor traffic, signs, and road conditions [3].

Table-1: Attack vectors in the sensor layer on vehicle



Attack Vector	Access	Sensor Type	Description
Sensor Components	Physical	Active, Passive	Sensors can be physically tampered with or destroyed.
Receiver	Remote	Active, Passive	Attackers can transmit illegitimate signals to a sensor's receiver.
Emitter	Remote	Active	Emitted signals can be eavesdropped and recorded.
Side Channel	Remote	Active, Passive	External stimuli can be directed at the sensor's transducer to disable sensor functionality.

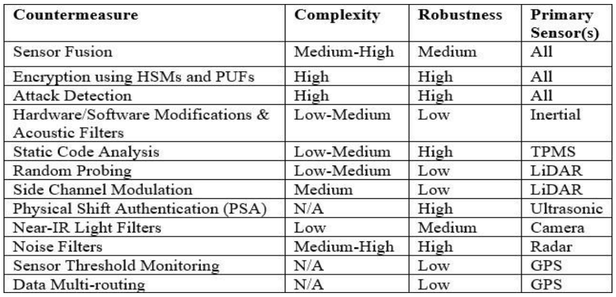
B. Environment and vehicle dynamics sensors

Detectors in the sensing layer are classified into two types: car dynamics sensors and environmental sensors. Automobile dynamics sensors track the car's state, while environmental sensors sense its surroundings. Most vehicle dynamics sensors (receivers) are inactive, whereas environment sensors are active (emitters and receivers), resulting in a larger attack surface. Environment sensors detect external elements and offer an overall location using Lidar, Camera, ultrasonic sensors, RADAR, and GPS receivers. The DAS makes use of this data to enhance vehicle safety [3]. Vehicle dynamics sensors monitor the car's three- dimensional operation, including velocity, acceleration, and turn rates. In-vehicle telematics sensors, such as tyre pressure monitoring systems (TPMS) and inertial sensors, track operating data [5].

C. Attack Vectors and Defenses

The sensor layer, which is critical to vehicle functioning, is vulnerable to attacks from both physical and remote interference. The damage or disrupt sensors crucial to its operation on the other hand, remote tampering employs a range of strategies, such as roadside attacks, front/rear/side assaults, and landscape modification, all of which try to deceive car sensors by modifying the surroundings [1]**.** Inside the area of remote manipulation, two unique attack vectors have been established inside the sensing layer: the normal channel, which serves as the physical interface for sensor input and emissions, and the side channel, which involves stimuli detected incorrectly by the sensor. Physical and distant assault vectors require strategic considerations for comprehensive defense. To effectively fight against vehicle sensor exploitation, a set of strong security measures must be in place to ensure sensor data's continuous availability, authorized access, confidentiality, freshness, and integrity. These defensive measures become increasingly important as vehicle sensors gradually replace human observation, influencing judgements with direct consequences for both motorists and pedestrians.

Table-2: Comparison of vehicular sensor countermeasures



Countermeasure	Complexity	Robustness	Primary Sensor(s)
Sensor Fusion	Medium-High	Medium	All
Encryption using HSMs and PUFs	High	High	All
Attack Detection	High	High	All
Hardware/Software Modifications & Acoustic Filters	Low-Medium	Low	Inertial
Static Code Analysis	Low-Medium	High	TPMS
Random Probing	Low-Medium	Low	LiDAR
Side Channel Modulation	Medium	Low	LiDAR
Physical Shift Authentication (PSA)	N/A	High	Ultrasonic
Near-IR Light Filters	Low	Medium	Camera
Noise Filters	Medium-High	High	Radar
Sensor Threshold Monitoring	N/A	Low	GPS
Data Multi-routing	N/A	Low	GPS

1. Availability: Sensor data should always be accessible as it is used to make decisions that affect the safety of drivers and pedestrians.
2. Authorization: Only authorized sensors may gather and send information about the vehicle and its surroundings.
3. Frequent collection of sensor data ensures its accuracy and freshness.
4. Integrity: Sensor data should not be altered during transmission to other nodes.

Table 2 provides a detailed overview on protective measures adapted for various sensors in autonomous cars. These metrics are classified according to complexity, ranging from simple hardware and software needs to more complicated circuits and advanced software. The table assesses the resilience of each countermeasure, indicating its efficacy against various assault scenarios. For instance, noise filters emerge as very effective, giving protection against a range of threats, including jamming and spoofing/relay assaults [3].

III. Vehicle Dynamic Sensors

Automobile dynamics sensors, such as magnetic encoders, inertial sensors, and Tyre Pressure Monitoring Systems (TPMSs), are crucial in providing observations on an automobile's status. This section outlines potential attacks on automobile dynamics sensors, as well as precautionary methods that automakers can employ to prevent and identify unauthorised manipulation [5].

A. Magnetic encoders.

Magnetic encoders, or wheel speed sensors, detect the rotational velocity exhibited by a vehicle's gear or tyre. Wheel speed sensors, which use magnetoresistance Integrated Circuits (ICs) or Hall, are extensively implemented in anti-lock braking systems (ABS) and indirect TPMSs. These sensors compute pressure differences by analyzing changes in rotating speeds [3].

1) Attacks:
Disruptive assault: In an assault, a malicious actor disturbs the by placing an electromechanical actuator somewhere between the steering wheel speed sensors—which are visible beneath the vehicle's body—and the anti-lock brake tone ring's magnetic attraction. Spoofing attacks use unauthorized access to a system to misrepresent information shielding the original magnetic field and dramatically influencing the sensor's output [6].

2) Countermeasures:
Physical Challenge-Response Authentication protects either inductive active sensors or magnetic encoders by implementing security procedures prior to digitizing the sensor response, assuring unpredictability via non-zero delays. Adjustments to PyCRA. Following the successful demonstrations of PyCRA bypass, adjustments were proposed to improve resistance against spoofing assaults, which included phase changes in situations.

IV. Vehicle Environmental Sensors

Environment sensors are essential for delivering measurements about a vehicle's surroundings. These sensors include a variety of technologies such as LiDAR systems, ultrasonic sensors, cameras, and GPS sensors.

A. LiDAR

LiDAR devices use laser scanning to generate a three- dimensional map of their environment. There are two types of LiDAR systems: scanning and solid-state [8]. Scanning LiDARs use rotating laser transceivers, but solid-state LiDARs can map without rotation. Scanning LiDARs, which are widely used nowadays, generate laser pulses while rotating to survey the vehicle's surroundings. Adaptive Cruise Control (ACC) and Collision Avoidance systems rely on the three-dimensional, 360-degree vision provided by LiDARs.

i. Attacks:
Replay Attack: Attackers can capture and replay LiDAR signals, leading it to map non-existent objects. Extends replay assaults by sending signals to a separate area and then relaying them back to the LiDAR, compromising its precision [3].

Blinding Attack: Injecting an external light source with the same wavelength as LiDAR pulses to produce saturation and refuse service to the vehicle.

Spoofing Attack: Causes LiDARs to identify non-existent objects, potentially overestimating or underestimating distances [9].

Jamming Attack: Returns light to the LiDAR's scanner unit, impairing its operation, utilizing the same frequency band as the laser.

Denial-of-Service Attack: Floods LiDARs with phoney objects via jamming or spoofing, destabilizing the system if the injected items exceed the LiDAR's tracking capability.

ii. Countermeasures:
Modulating the LiDAR laser using side-channel information to prevent attackers from sending misleading reflection signals [5].

Using signals with diverse wavelengths to make it difficult for attackers to target many wavelengths at once.

Using random probing to change the time interval between laser pulses, making it harder for attackers to forecast when to insert a bogus pulse.

Using numerous probing instances to identify random jamming and narrow the attack window.

Increase the number of objects monitored simultaneously by the LiDAR sensor to prevent denial-of-service assaults.

B. Ultrasonic Sensor

This detect surroundings then compute their space from the automobile by sending ultrasonic signals and monitoring how long it takes for them to be reflected. These sensors are commonly employed for low-speed operations such vehicle parking and serve an important role in improving driver assistance systems [3].

i. Attacks:
Blind Spot Exploitation Attack: By exploiting the shortcoming that ultrasonic sensors may not detect very thin items in their blind areas, attackers might place thin objects in the blind spot of a reversing vehicle, resulting in a collision [3] [6].

Sensor Interference Attack: Attackers can disrupt genuine sensor readings by positioning their ultrasonic sensors opposite the vehicle's sensors, resulting in signal overlap and misunderstanding.

Cloaking Attack: Attackers utilize sound-absorbing materials to disguise items from ultrasonic sensors, preventing detection.

Physical Tampering Attack: By physically covering an ultrasonic sensor's receiver and transmitter, attackers can impair its operation.

Acoustic Cancellation assault: This assault attempts to remove authentic ultrasonic transmissions by sending an unauthorized signal with the opposite phase.

ii. Countermeasures:

Advanced algorithms that combine 3D-CAD geometry with computer vision techniques, such as instance segmentation, color edge recognition, and backdrop removal, can improve real-time blind spot identification [3].

Physical Shift Authentication (PSA) randomly generates ultrasonic signal waveforms and accepts reflected signals only if they match the randomized waveform. Continuous frequency shifts avoid jamming assaults. Receiving signals with suspicious pulse lengths to protect.

C. Camera

Cameras play an important part in driverless cars, allowing the vehicle to recognize in low visibility conditions, and assisting drivers with parking by revealing nearby obstacles, collision avoidance through the tracking of nearby objects using sensor data, and validating information from other sensors [3].

i. Attacks:
Blinding Attack: This form of attack disables the vehicle's camera sensors by sending a powerful laser beam at the camera. The attacker uses the resulting increased tonal values to conceal the camera feed, causing full blindness in vehicular sensory inputs. This might cause irregularities in the vehicle's functioning or even activate emergency brakes [3].

ii. Countermeasures:
There are many solutions to protect cameras from blinding and auto-control assaults. These include combining during daytime hours and using photochromic lenses to filter certain wavelengths of light. Furthermore, Rangesh and Trivedi investigate a "full- surround" Multi-item Tracking (MOT) framework that uses early fusion and ground-truth pictures to monitor things in real-time and inform the driver if an item is spotted, therefore reducing blind spots [3].

D. Radar

Radar sensors use electromagnetic waves to determine the distance between adjacent objects by measuring the duration between signal transmission and reception.

Jamming Attack: Attackers can disrupt radar sensors by jamming them with a signal in the same frequency range. Signal jamming lowers the sensor's signal-to-noise ratio, limiting its capacity to identify surrounding objects.

Spoofing/Relay Attacks: Malicious actors fake signals and repeatedly retransmit a previously lawful transmission. Digital Radio Frequency Memory (DRFM) repeaters are used to store and replay signals, deceiving the radar into believing they are authentic.

Yan et al. propose combining data fusion with assault detection. Identify and reduce the impact of fake data supplied at random places. Another study employs a Spatio-Temporal Challenge- Response (STCR) technique using MIMO antennas and multiple beamforming to continuously explore the surroundings, identify reflected signals, and eliminate malicious signals from distance computations if they surpass a noise threshold [6].

E. GPS

Connected and autonomous cars use the Global Positioning System (GPS) to determine their position identification and geographic coordinates. GPS satellites provide navigation signals, which use the messages' transmission and arrival timings to compute their distance to the satellites [3]. However, because GPS signals lack authentication and encryption, the communication is vulnerable to assaults. Assaults against GPS systems in automated cars, as well as assaults on camera sensors, are considered high cybersecurity priorities [5] [6] [3].

Jamming Attack: Jamming disrupts the sensor signals, making it impossible to identify the vehicle being jammed. Pett and Shlad claim that GPS jamming is a simple assault, made easier by the low cost and widespread availability of GPS jammers, the vehicle's receiver is unable to distinguish the genuine signal [3]. May interfere with the GPS receiver, calculating bogus positions and timings, or transmitting data to disrupt connection between the GPS receiver and satellites, preventing the device from identifying its position. Spoofing assaults may act as a prelude [1].

Attackers can tamper with GPS data to advertise the quickest path to the destination node, allowing them to modify routing pr otocols and discard crucial packets, disturbing network topology [2]. Grey-hole attacks, a variation, vary between regular behavior and random packet drops, making them difficult to detect. Petit and Shladover recommend using inertial sensor measurements to prevent GPS jamming assaults. Khanafseh et al.

V. CONCLUSION

In conclusion, the future of self-driving vehicles has enormous potential as the automotive industry works tirelessly to improve road comfort and safety. The continuous study and development of fully autonomous cars emphasizes the critical role that sophisticated sensors play in determining their usefulness. With each car possibly outfitted with over 200 sensors, sophisticated onboard infotainment systems, and powerful cloud-based telematics, vehicle makers, vendors, and consumers must priorities data privacy and security [1]. When the landscape of cyber threats evolves, particularly when cyber-attacks emerge as a form of warfare, the incorporation of cutting-edge technology such as machine learning and block chain becomes critical to strengthening cybersecurity solutions. Recognizing this paradigm change, guidelines presented in an IEEE paper provide a complete framework for addressing cyber dangers across several dimensions, such as legal and legislative views and human factors [3].

Automotive original equipment manufacturers (OEMs) must be prepared to deal with unpleasant, disruptive, and possibly catastr ophic situations that arise because of the deployment of these technologies. Swift policy formulation and engagement with key parties, such as regulators, industry, government agencies, national labs, and non-profit organizations, are critical for developing legal and responsibility procedures. Furthermore, the lack of regulatory organizations regulating malfunctions or insufficient deployment of ML/AI technologies emphasizes the importance of establishing coordinated data warehouses funded by both governments and enterprises. Like programs like as the Waymo Open Dataset, these data warehouses should help to develop national or worldwide standards for feature engineering, processing, and storage [1] [3].

VI. REFERENCES

[1] “Waypoint - The official Waymo blog,” 2020. [Online]. Available: https://blog.waymo.com/

[2] “Tesla Autopilot AI,” 2020. [Online]. Available: https://www.tesla.com/autopilotAI

[3] IEEE SENSORS JOURNAL,” Cybersecurity attack in Vehicular sensor” 2020

[4] “Aptiv - CTO Blog,” 2020. [Online]. Available: https://www.aptiv.com/newsroom/cto- blog/253985928

[5] “Self-driving cars take the wheel,” *MIT Tech- nology Review*,feb 2019.[Online].Available: https://www.technologyreview.com/2019/02/15 /137381/self-driving-cars-take-the-wheel/

[6] S. International and Synopsys, “Securing the Modern Vehicle: A Study of Automotive Industry Cybersecurity Practices,” Tech. Rep., 2019.