International Journal of Electrical, Electronics and Data Communication, ISSN(p): 2320-2084, ISSN(e): 2321-2950
Volume-8, Issue-4, Apr.-2020, http://iraj.in

VULNERABILITIES IN THE NAVIGATION SYSTEM OF CONNECTED AUTONOMOUS VEHICLES

DIMAH ALMANI

Shaqra University, Shaqraa, Saudi Arabia
E-mail: Dalmanea@su.edu.sa

Abstract - Advanced driver assistance systems are advancing at a rapid pace and all major businesses started investing in developing the autonomous vehicles. However, reliability and security are still uncertain and debatable. Navigation is an essential part of a mobile robot, especially the ability to self-navigate is of immense importance to an autonomous vehicle. For this purpose, it is necessary for the vehicle to know its current position as well as an area of a map it has to navigate. GPS provides the required position data and a compass gives the current heading. This data in conjunction with a list of waypoints obtained from the map is used to calculate the required correction in heading. This is then used to obtain the steering angle to navigate the vehicle. For example, a vehicle is compromised by the attackers. An attacker can accelerate, control brake, and even steering which can lead to catastrophic consequences. This paper presents a very brief and short overview of predictable attacks on autonomous vehicle software and hardware and their potential implications.
steering angle to navigate the vehicle. For example, a vehicle is compromised by the attackers. An attacker can accelerate, control brake, and even steering which can lead to catastrophic consequences. This paper presents a very brief and short overview of predictable attacks on autonomous vehicle software and hardware and their potential implications.

Keywords - Attacks, Autonomous, Connected, GPS, Security, Vehicle, Vulnerabilities

I. INTRODUCTION

Connected and Autonomous Vehicles (CAVs) offer the prospect of significant benefits including improved safety, reduced traffic and emissions, and an enhanced the driving experience. To function effectively, CAVs require GPS as well as multiple sensors (LiDAR, radar, camera) working in concert to make both short-term (i.e. safety-related) and long-term (i.e. planning) driving decisions. In addition to being reliable, accurate, and trustworthy in a wide range of often difficult environments and driving situations, GPS and sensors must also be able to detect and fend off intentional or unintentional attacks that may disrupt the automation system.

An ever-increasing number of wireless applications rely on GPS signals for navigation, localization, and time synchronization. Despite their widespread use, GPS signals are exposed to spoofing attacks which can cause GPS receivers to accept false range, location, and timing information as accurate. This research investigates the requirements for successful GPS spoofing attacks on CAVs with GPS receivers. This paper identifies the areas and precision that attacker needs to generate its signals in order to successfully spoof the receivers. For example, any number of receivers may be spoofed to one arbitrary location; however, the attacker is limited to only a few transmission locations when spoofing a group of receivers while also preserving their constellation.

To detect objects that including an obstacle on the road, all CAVs use Light Imaging Detection and Ranging (LiDAR). Any attack that tricks sensors into thinking an object is in its path can trigger an emergency brake or at least a fake warning. One possible attack relays the original signal sent from the target vehicle LiDAR from another position to create artificial echoes, making real objects appear closer, farther, or otherwise other than their actual locations. Extended attacks can be used to create multiple false objects and structures, captures the LiDAR signal, duplicates it, and spoofs the LiDAR with the intention of re(p)laying objects and controlling their position. Cameras, which are used to detect traffic signs and other significant objects, can also be attacked. For example, they can be blinded by high intensity light which overexposes the image and hides the object from the autonomous system, or by bursts of light that confuse the camera controls and in some cases, the camera never recovers. This paper will also examine methods for attacking CAV sensors.

Moreover, this paper also proposes a novel idea for mitigating a known data-storage issue in CAVs. A weakness of CAVs technology is the volume of data and questions of how to handle such large quantities of data within the limited size and space available in a traditional vehicle. This paper presents a cloud based CAVs alternative that can alleviate this data storage problem. The idea is not to store any data in CAVs. Instead, data will be uploaded to and downloaded from the cloud as needed. This approach relies on a cloud-based infrastructure and diminishes the need to store significant amounts of data.

This paper didn't just discover the vulnerability and then toss the problem to the automakers and their suppliers. Instead, it proposed software and hardware countermeasures to improve sensors resilience against these attacks. At On-Board Security, our purpose is to make both autonomous and connected vehicles as resistant to cyber-attacks as possible. The hope is that paper like this, will identify these potential attacks for automakers so they can make more robust systems and avoid potentially life-threatening situations for their clients.

The current research focuses on navigation in CAVs, identifies certain technological challenges that must be met, and suggests some approaches to meeting these. This research will focus on the security challenges arising from the use of GPS, sensors, and the cloud in CAV navigation systems.

This paper is structured as follows. Section 2 explains how the CAVs navigation system works. Section 3 addresses system drawbacks and vulnerabilities with a focus on identifying security vulnerabilities and knowledge gaps associated with the navigation system. Section 4 discusses means of eliminating vulnerabilities and protecting against cyberattack. The paper concludes with a discussion of what has been achieved, suggestions regarding how some of the knowledge gaps might be addressed, and some open questions for the CAV community to consider.

II. CAVs NAVIGATION SYSTEM OVERVIEW

Navigation systems are designed to identify a recommended route to a selected destination based on global factors such as distance and estimated time required to travel based on such conditions as allowed speed and traffic conditions. Advanced control systems interpret sensory information to determine appropriate local navigation paths, based on such conditions as local obstacles and relevant signage. Some autonomous vehicles update their maps based on sensory input, allowing vehicles to be tracked even when conditions change or when they enter uncharted environments. For any mobile robot, the ability to navigate in its environment is a critical capability. In general, the navigation task comprises three basic elements: (1) localization – the robot's ability to determine its own position and orientation within a global reference frame; (2) route – the computation of an adequate sequence of motion commands to reach the desired destination from the current robot position; and (3) control – who or what is guiding the vehicle [1]. The planned path is followed by the robot's feedback control. This controller includes global path preplanning as well as reactive obstacle avoidance. Autonomous cars as shown in Fig I sense their surroundings with techniques including GPS, radar, lidar, camera, and cloud-based references.

A. Global Positioning System (GPS)

Navigation systems take the current position of the vehicle as the source and obtain the destination point from the passenger. The system then computes the best path to the destination, extracting the location from the graph and sending the coordinates to the CAV. This technique follows the coordinates using GPS and compass. GPS and sensors technology can provide decimeter-level accuracy of position, and the navigation system ensures a vehicle stays in its lane and at a safe distance from other vehicles and obstacles. If the GPS signal is lost, the inertial navigation system must obtain the current coordinates independently. Without any human intervention, an auto-navigational vehicle model can route itself through known or pre-programmed coordinates autonomously. GPS-based CAVs demonstrate the feasibility of using a low-cost strap-down inertial measurement unit (IMU) to navigate between intermittent GPS fixes [2].

GPS-based CAVs used real-time geographical data received from a number of GPS satellites to calculate latitude, longitude, speed, and course to facilitate navigation [3]. GPS actually serves two purpose in CAVs, the first being its use for navigation and the second being the ability to share information outside the CAV. Ride-sharing apps like Lyft and Uber, car-sharing, usage-based insurance applications, parking applications, and dynamic toll charging are all based on the ability to know and share the location of the car at all times. GPS ultrasonic sensors offer enough accuracy for each of these applications by providing location coordinates. For these reasons, GPS receiver will most likely remain a critical component in CAVs.

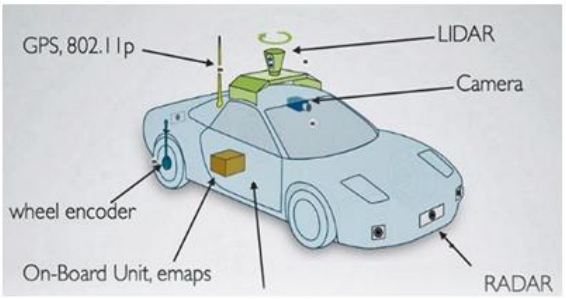

Figure I

GPS is a federally operated service that offers global positioning, navigation, and timing (PNT) free of charge. GPS has three main elements that all work in conjunction to produce the PNT results [4]: (1) a constellation of satellites that operate in six separate orbits around Earth and transmit signals to GPS receivers with each satellite's position and time; (2) the control segment that monitors and controls the satellites; and (3) the GPS receivers that pick up the satellites' signals and use them to compute their 3D position and time.

Two classes of signals are broadcast by each GPS satellite: encrypted signal for military uses and a non-encrypted signal for civilian uses. Upon receipt of a satellite's signal, a GPS receiver produces an internal copy of the code and compares its copy with that of the satellite in order to determine the clock offset (δ) and then infer the pseudo-range (R) without requiring a precise local clock:

$R = d + \Delta$ and $\Delta = c\delta$

where d is the range and c is the speed of light.

With four unknowns, 3D position, and timing, at least

four satellites should be in the line of sight due to data noise:

$$(x - x^2)^2 + (y - y^s)^2 + (z - z^s)^2 = (R - \Delta)^2 \quad (1)$$

where (x, y, z) is the GPS receiver's position, (x^s, y^s, z^s) is each satellite's position.

Solving the set of four equations (1), the GPS receiver determines its own 3D-position (x, y, z) and its own clock error ($\delta = \Delta/c$), together called a 3D-fix [5].

The flexibility and reliability of GPS is used in technologies affecting all sectors of modern life. Electronic devices, from phones to automobiles, employ GPS technology. Time synchronization for power grids and financial markets, global positioning to track cargo convoys in real time, and navigation in daily travel all reply on GPS [6].

B. Sensors

Sensor technology has become ubiquitous and has attracted much attention in recent decades. Besides monitoring vehicle and marine activity, sensors have been deployed in areas such as healthcare, agriculture, and forestry [7]. In CAVs, sensor technology supports the development and design of a wide range of applications for safety, traffic control, and entertainment. Recently, federal regulation in the United States outlined certain requirements in the manufacture of vehicles and the implementation of intelligent transportation systems, including sensors and actuators, a component of a machine that is responsible for moving and controlling CAVsystems such as tire pressure sensors and rear-view visibility systems [8]. Sensors aim to improve road safety, increase passenger satisfaction, and reduce traffic congestion. Other sensors are optionally installed by manufacturers to monitor the performance and status of the vehicle, provide higher efficiency, and assist passengers. Currently, the average number of sensors in a vehicle is around 62–100, but in CAVs, the number of sensors might reach 200 [9]. Sensors may be classified according to their location in the vehicle: chassis, powertrain, and body [10]. Another work classifies sensors in CAVs based on the type of application the sensor is intended to support. Alternatively, [11] identified four categories of sensors: safety, diagnostics, convenience, and environmental monitoring. In this article, we add two additional sensors categories for driving monitoring and traffic monitoring, as shown in Table I.

Ultrasonic sensors use a form of sonar to identify how far a vehicle is from an object, alerting the vehicle to take the right action when it gets closer than a set threshold. Electromagnetic sensors alert the passenger when an object enters an electromagnetic field created around the front and back bumpers. Proximity sensors have been used to support a system based on a rectangular capacitive proximity-sensing array for occupant head position quantification in order to meet the guidelines of the Insurance Institute for Highway Safety (IIHS) [8]. Often, these kinds of sensors are affected by temperature and humidity, reducing their accuracy, and in low-light environments, sensors can only detect a vehicle if its headlights and taillights are on and are clearly visible. Radar and laser sensors continually scan the road for potential front, rear, and side collisions, then allow safety applications to adjust throttle. Additionally, CAV activates brakes to avoid potential collisions or risk situations, using radio waves to determine the distance between obstacles and the sensor. In addition, the Inertial Navigation System (INS) uses gyroscope and accelerometer sensors to determine the vehicle's parameters such as vehicle position, velocity, and orientation. INS is used in conjunction with GPS to improve accuracy. Radar and speed sensors are used in applications that warn the passenger of potential danger when changing lanes or if obstacles are detected.

Category of Sensors	Description	Example
Safety	Form the basis of safety systems and focus on recognizing accident hazards and events almost in real-time.	Micro-mechanical oscillators, speed sensors, cameras, radars and laser beams, inertial sensors, ultrasonic sensors, proximity sensors, night vision sensors, haptic.
Diagnostic	Focus on gathering data for providing real-time information about status and performance of the vehicle for detecting any malfunction of the vehicle.	Position sensor, chemical sensors, temperature sensors, gas composition sensors, pressure sensor, airbag sensor.
Traffic	Monitor the traffic conditions in specific zones, gathering data that improves the traffic management.	Cameras, radars, ultrasonic, proximity.
Assistance	Responsible for gathering data that provide support for comfort and convenience applications.	Gas composition sensor, humidity sensors, temperature sensors, position sensors, torque sensors, image sensors, rain sensors, fogging prevention sensors, distance sensors.
Environment	Monitor the environment conditions, offering drivers and passengers alert and warning services that are used to enhance their trips.	Pressure sensors, temperature sensors, distance sensors, cameras, weather conditions.
User	Focus on gathering data that support the detection of abnormal health conditions and behavior of the driver that can deteriorate the driver's performance.	Cameras, thermistors, Electrocardiogram (ECG) sensors, Electroencephalogram (EEG). sensors, heart rate sensor.

Table I

LiDAR has been an essential factor in the evolution of CAVs. LiDAR enables CAVs (or any robot) to observe the world with continuous 360-degree visibility and highly accurate depth data. LiDAR sensors continually emit beams of laser light; then measure the time it takes for the light to return to the sensor. In CAVs, sensor integration with other components and the lack of widely accepted standardization among brands are obstacles to their broad adoption.

In CAVs, multiple cameras are used in concert to allow detection of lane lines and road signs. In addition, cameras can monitor vehicle's posture, and activity to detect abnormal conditions, such as signs of fatigue, or sense if another vehicle or potential obstacle is behaving erratically, such as pedestrians crossing suddenly in front of the vehicle or another

car veering out of its lane on the road). These cameras have high resolution, seeing in enough detail to recognize a passenger's arm sticking out to signal a turn, but they can only see what the sun or headlights illuminate, so they have the same trouble in low light and bad weather that humans might in detecting danger. Despite limitations, cameras are used to execute night-vision assistance applications to help passenger see farther down the road and detect objects such as animals, people, or debris in the road that might cause a risky situation or an accident. Researchers are presently exploring use of machine-learning techniques to make better use of real-time sensor data.

Generally, CAVs technology is processed by artificial intelligence (AI) algorithms that enable CAVs to steer in a manner that is more accurate and safer than human drivers are capable of. Furthermore, pattern recognition processing in CAVs is utilized to assist in the recognition of landmarks and street signs by registering their positions on the map. As showed in Fig II, the AI-processing "brain" can access detailed map databases either through a network connection or local storage.

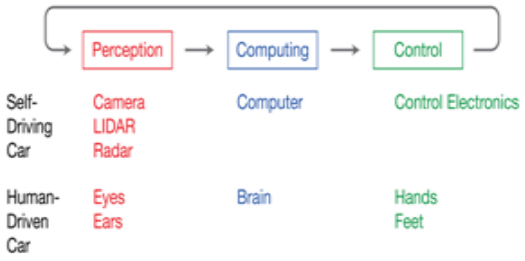

Figure II

C. Cloud

A GPS-based system includes four modules. In addition to the three GPS sensors mentioned previously, the cloud serves as an essential fourth module: the backend provider of computation and storage. Every auto-vehicle generates about one gigabyte of data per second [12]. CAVs need roadmaps, computer code, and huge data to support self-driving vehicles. Using the cloud to store data and provide computation for CAVs and the driving environment is one potential solution.

Consider an example of the cloud's role in GPS tracking systems. A GPS receiver equipped on a vehicle connects with a set of at least four satellites in its current view and geometrically calculates its 3D position on the globe and the time from the signals received. The microprocessor in the receiver relays this data via wireless communication, such as cellular service, to a cloud server. The information is stored and processed by a monitoring center tracking the vehicle in real time.

In the Google's self-driving vehicle, all the data resides inside the vehicle. Switch on the vehicle and the vehicle takes the code, gets the maps ready, combine them with the live images and then begin the drive. The data here is pulled from the cloud which means the code also. When the vehicle starts moving, the on-board computer gets connected to the network, whichever is available: Wi-Fi,3G, or 4G.

To illustrate, this process starts the web console and asks for the authentication from the user. The user signs in with the username and password that registered with the cloud service provider. Then, the user inputs in detail the location to where he needs to drive. After that, the software downloads the code to process the information, takes the pre-recorded information from the cloud that is just needed to go to that locations, the world maps and begins processing. Everything will be still in the control of user as how it is when the data is in the vehicle. The best benefit is that since nowadays V2V is gaining popularity the clouds will interact and make CAVs safer.

To fully understand the storage and computational requirements to support self-driving vehicles, it is necessary to examine the basic real-time information requirements of autonomous vehicles and the environment. Moreover, the demand for cloud-based support is likely to grow and change in character as the safety and functional requirements of autonomous vehicles become better defined and more challenging with time.

More generally, to understand the data storage requirements of CAVs, it is necessary to examine the basic real-time information requirements of autonomous vehicles and the environment. Every auto-vehicle generates about one gigabyte of data per second [12]. CAVs need roadmaps, computer code, and huge data to achieve 'humanless' driving. Using the cloud to store data needed for CAVs is one potential solution. The cloud would store data on traffic rules, roadmaps, live traffic data, signal information, and all other data required by CAVs. As the management consulting firm Guerrero-Ibáñez, Zeadally, Castillo (2018) [13] state, CAVs technology processes three different types of data in a so-called hybrid approach: camera, light detection and ranging LiDAR, and radar data. Those technologies can capture basics of the environment to generate a combined data pool. This data must be processed and then stored for simulation purposes and model training [14]. In addition, these three data classes are supplemented by ultrasonic sensor data and vehicle motion data.

As showed in Figure IV, when the passenger's authentication is complete, he can input the region to which the vehicle should take him and the exact location. In theory, only the data needed to take the vehicle to the specific site indicated by the passenger needs to be saved to the vehicle's computer, thus avoiding the need for the vehicle to carry a massive amount of data on the go. The cloud premise is based on the assumption that there is persistent network connectivity and sufficient storage available in the

vehicle to back up the data if it is known in advance that the vehicle will be driving to a location with limited/no network availability.

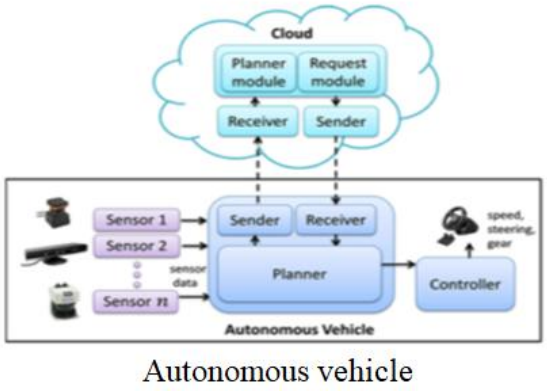

Figure III

III. ATTACKS EXPLOITING CAVs VULNERABILITIES

As explained, CAV navigation systems use the following devices: GPS, millimeter wave (MMW) radar, LiDAR sensor, ultrasonic sensor, and camera sensor. Also, they use the cloud for off-vehicle computation and storage. Cloud connectivity and storage should protect current and future CAVs against sensor attacks. Vulnerabilities and attack methods are briefly described below. Potential countermeasures are also noted where possible.

A. GPS

GPS is a space-based radio navigation system that provides geolocation and time information. Since the main purpose of GPS is to identify location and navigate, the system needs to be highly accurate. To ensure continual and uninterrupted access to GPS data, there must be enough well-positioned public access GPS satellites. In research conducted by Zeng et al. (2018) [15], GPS in navigation systems consists of 31 satellites in medium Earth orbit and each satellite is equipped with a synchronized atomic clock. Each satellite continuously broadcasts GPS information using coarse/acquisition *(C/A)* codes on the L1 band at 1575.42 MHz. The publicly available data access and its transparent architecture can be exploited by hackers either to manipulate the data to control the routing of the vehicle or to provide incorrect directions [16]. This exposes the passengers to security and safety risks. According to [17], GPS signals can be disrupted via jamming (elimination of the signal), which prevents the reception of the signal by a receiver, usually by injecting enough noise into the receiver that it can no longer pick out the actual signal from all the noise, or via spoofing, which is much more complicated: a spoofing signal attempts to convince a receiver that it is receiving a legitimate GPS signal. This requires producing a sufficiently powerful fake signal that overwhelms the real signal at the receiver.

GPS-based CAVs are vulnerable to spoofing attacks. GPS spoofing attacks have two main phases. In the takeover phase, the hacker lures the victim GPS receiver to migrate from the legitimate signal to the spoofing signal. The takeover may be either by brute-force or smooth. In the former case, the attacker simply transmits the false signals at a high power, making the victim receiver unable to track the satellites and lock on to the stronger spoofing signals. In the latter case, smooth takeover starts by transmitting signals synchronized with the original ones and then gradually overpowering the original signal to cause the migration. The benefit of a smooth takeover is stealth because it will not generate abnormal jumps in the received signal strength. However, according to [18], smooth takeover needs specialized and costly hardware to track in real-time and synchronize with the original signals at the victim's location. In the subsequent control phase, the attacker manipulates the GPS receiver by either shifting the signal's arrival time or modifying the navigation messages [18].

Protecting GPS from spoofing is critical to integrity of the CAV navigation system. In conventional GPS, signal spoofing can be achieved easily using inexpensive equipment. Advanced spoofing technology will pose defense challenges even to very sophisticated receiver capable of protecting against more conventional attacks. There is no commercial anti-spoofing GPS system available in the market. Hence, there is a need for more research and development in spoofing defenses, especially concerning the question of how to recover accurate navigation after the detection of an attack.

B. Sensors

CAV sensors, which include inertial measurement units (IMUs), LiDAR, radar, and cameras, are used to generate a map of the vehicle's environment for localization, obstacle detection and avoidance, and navigation. These sensors are vulnerable to attacks such as jamming and spoofing.

IMU: According to [19], IMU is the combination of accelerometers and the gyroscopes that delivers vehicle velocity, acceleration, and orientation data. It also monitors changes in environmental dynamics such as road gradient. If sensor data is altered to provide, for example, a false road gradient reading, vehicle motion may be impacted; e.g., moving too slowly or quickly on hilly grades, endangering passengers in this and other vehicles.

LiDAR: LiDAR is a surveying technology that measures the length of time a pulse of light travels to determine the distance between the sensor and an object. It can only see things that are reflected by the signal. If the signal does not return due to absorption, refraction, or range limits, LiDAR will 'see' nothing there. Much of a 360-degree view around us would often be classified as 'nothing. Reflective objects can confuse a laser beam since they can appear in the

field-of-vision when they should not, a major issue for collision avoidance systems (CAS). Misinterpreted data may indicate that objects located behind the vehicle are, for example, in front. Moreover, some objects on the road are reflective by design. Lane markings reflect some light, and so will be visible in the LiDAR image. The main purpose of an attack on LiDAR is to generate noise, fake echoes, or fake objects. A work conducted by Stottelaart (2015) [20] demonstrates the potential for jamming LiDAR by directing back at the scanner unit light which is of the same frequency as the laser reflecting on the target. A similar attack was more recently demonstrated by researchers from the University of Cork (2017) [21].

Radio Detection and Ranging (RADAR): Tesla's autopilot detects the vehicle's surroundings in three different ways: radar, ultrasonic sensors, and cameras. Researchers attacked all them and found that only radar attacks have by far the greatest potential to cause high-speed collision [22]. A radar sensor can be classified by its operating distance ranges: Short Range Radar (SRR), 0.2 to 30m range; Medium Range Radar (MRR), 30 to 80m range; and Long-Range Radar (LRR), 80 to 200m range. Radar jamming and spoofing attacks use off-the-shelf hardware to cause system blinding and malfunction, which can potentially lead to crashes and impair the safety of CAVs. Attackers use jamming techniques to disrupt autonomous vehicles' short- and long-range wireless communications. Attackers can blind autonomous vehicle radar systems by jamming the radio frequency (RF) signals that the radar emitters send and receive using signal generators [23].

Monoscopic and Stereoscopic Cameras: Cameras are used for detection and recognition of lane lines, traffic signs, headlights, and other obstacles. The complementary metal oxide sensors (CMOS) used in such cameras can be partially disabled by the headlights of oncoming vehicles or by using high-powered flashlights. Camera failure or malfunction can lead to false positives (detection of nonexistent objects) and false negatives (failure to detect objects), both of which are safety concerns.

A camera sensor (MobilEye C2-270) tested by Petit et al. (2015) could be blinded by a laser and LED matrix, thereby confusing the auto controls. For the MobilEye C2-270, a simple and inexpensive laser pointer was enough to blind the camera and prevent detection of vehicles ahead. As far as we know, there is no commercial anti-blinding camera sensor available in the market.

B. CAVs Cloud and Network

According to Taha & Shen (2013) [24], Vehicular Ad-Hoc Network (VANET) is a sub-form of Mobile Ad-Hoc Network (MANET), which provides communication between vehicles (V2V) and between vehicles and road-side base stations to providing safe and efficient transportation. A vehicle in VANET is an intelligent mobile node capable of communicating with its surroundings and other vehicles in the network. The following will explain the challenges and vulnerabilities related to VANET in CAVs.

CAVs can be connected to smartphones, the cloud, and/or other devices to establish V2X communication. Communication channels between vehicle and smartphone are established through Wi-Fi, Bluetooth, and GSM protocols, which contain known bugs and vulnerabilities that might be exploited by attackers.

Connecting CAVs to a smartphone presents a risk as it is interacting with an external and unfamiliar device. For example, sending and receiving data from the cloud is a threat because the datacenter might be compromised, and then the vehicle is vulnerable to attack via the compromised datacenter connection.

The Dedicated Short-Range Communication (DSRC) protocol in V2V networks is a duplex communication protocol channel used particularly for automotive use. V2V network attacks compromise the communication system between the host vehicle and adjacent vehicles, used to control overtaking/passing, lane changing, etc. An impersonation attack is when a malicious vehicle connects to the host vehicle with false or spoofed identification and sends malicious data and/or captures sensitive data (Khan, 2017). V2V communication uses insecure and unencrypted protocols which leaves sensitive information like authentication keys vulnerable to attackers. In Vehicle to Infrastructure (V2I) network attacks, a vehicle may be connected with intelligent traffic signs and cellular network nodes that can be compromised, infected, and impersonated by an attacker, again providing access through a backdoor into the vehicle's network and ECUs.

IV. PROTECTING CAVs FROM JAMMING AND SPOOFING ATTACKS

Rendering fully autonomous vehicles safe and protecting autonomous vehicle technology for large-scale deployment requires more effective safeguards than those in existence today [25]. Improvements to receiver autonomous integrity monitoring and complementary and backup systems are necessary to adequately defend against jamming and spoofing attacks targeting navigation system based CAVs.

According to Thing & Wu (2016) [26], the more satellites involved in GPS localization, the smaller area of overlap, and the better the position fix will be. In theory, three satellites are enough for a position fix. However, in practice, four satellites or more are required to acquire an accurate latitude, longitude, and altitude fix. The following proposed countermeasures, for detection of suspicious GPS signal activity, take advantage of the difference in signal strength between the fake and true signals as received from space [26]:

Monitor absolute GPS signal strength: This

involves monitoring and recording average signal strength over time. If a comparison between observed signal strength and expected signal strength of 163 dBw (5 x 10-17 watts) passes a preset threshold, the GPS receiver alerts the passenger. This countermeasure is based on the idea that relatively unsophisticated GPS spoofing attackers will tend to use GPS satellite simulators. Such simulators usually provide signal strengths many orders of magnitude larger than any possible satellite signal at the Earth's surface. This is an unambiguous indication of a spoofing attack.

Monitor relative GPS signal strength: The receiver software can be modified to record and compare average signal strength from one moment to the next. An extremely large change in relative signal strength would be characteristic of a counterfeit GPS signal meant to override the true satellite's GPS signals. a counterfeit signal is detected if signal strength exceeds a preset threshold, an alarm would sound, and the passenger alerted.

Compare time: Some current GPS receivers do not have an accurate clock. By comparing timing data from an accurate, continuously running clock with the time derived from the GPS signal, GPS signal veracity can be verified. If the time comparison shows a deviation outside of a preset range, the passenger will be alerted to the possibility of a spoofing attack. Based on the Vulnerability Assessment Team (2011) [27], precise clocks may be small and inexpensive and operate on very little power.

Compare time intervals: With many of GPS satellite simulators, the time between the artificial signal from each satellite and the next is a constant. This is not the case with real satellites. For example, the receiver can pick up the true signal from one satellite and then a few moments later pick up a signal from another satellite. With the satellite simulator, the receiver can pick up signals from all the "satellites" simultaneously. This is an exploitable feature of the satellite simulator that can be used to determine whether signals are authentic.

Monitor satellite identification codes and the number of satellite signals received: GPS satellite simulators transmit signals from around 10 satellites, more than the number of real satellites that can be regularly detected by a GPS receiver at a specified time. Several commercial GPS receivers display satellite identification data but do not record this information or compare it to previously recorded data. Tracking both the number of satellite signals received and the satellite identification codes over time will prove helpful in determining whether foul play may be afoot. This may be especially helpful in the case of an unsophisticated spoofing attack in which the adversary does not attempt to mimic the exact satellite constellation at a specified time.

CAVs' LiDAR technology is capable of quickly generating 3D maps of the environment, making it possible to develop a computational model used for object recognition and trajectory planning [28], [29]. However, this technology is not ideal for monitoring the speed of other vehicles in real time. This technology has been shown to be a viable assistance in CAVs, but as there is no guarantee of the validity of 3D model, it is vulnerable to spoofing and jamming with low-cost hardware. Research conducted by Stottelaart (2015) [20] demonstrated the potential for jamming LiDAR by shining light back at the scanner unit with the same frequency as the laser reflecting on the target. In addition to compromising a LiDAR laser using low-cost hardware (raspberry Pi and a low-power laser), and overwhelming the LiDAR sensor, which prevented the CAVs from moving, they also tricked the CAVs' control unit into believing that a large object was in front of the vehicle, forcing the control unit to stop the car.

Techniques to mitigate the risks of these attacks involve utilizing varying wave lengths to decrease the potential for jamming and spoofing attacks that use simple, off-the-shelf devices. Stottelaart's work also included the use of V2V communication to share measurements collaboratively across vehicles [20]. However, this raises a new threat: the potential for compromised measurement to be replicated beyond the single compromised car. Another, and more feasible, technique is to implement random probing. In this mitigation technique, the device frequently changes the interval between scanning speeds to make it difficult for the hacker to synchronize their laser to the correct frequency.

In CAVs, cameras used to help determine depth are often employed in tandem with other sensors. For example, the Google Driverless Car combines LiDAR with Enhanced Maps (Emaps) and stereovision for greater road-scenery analysis [30]. There are many other applications of cameras in CAVs, such as traffic sign recognition, lane detection [31], [32], and headlight detection [33]. The research conducted by Parkinson, Ward, Wilson, and Miller (2017) [2] highlights sophisticated image analysis techniques to recognize objects of interest. For example, planning a path through an identified lane requires detailed mathematical modelling, as demonstrated by Cheng et al. [2].

The radar system is often paired with sonar in at least some CAVs, and the front and back bumpers of CAVs feature radar units. While radar works up to 200 meters away, sonar is only suitable for 6 meters. They both have a narrow field of view, so the vehicle knows that the situation is hazardous if another vehicle crosses both radar and sonar beams. This signal could be used to swerve, apply the brakes, or apply pre-tension to seatbelts.

Conventional vehicles use radar to warn passengers of an impending impact or even apply the brakes to prevent one, but CAVs use radar to adjust the throttle and brakes continuously. The system is an adaptive cruise control that always considers the movement of

other vehicles and features of the surrounding area.

To strengthen CAVs cybersecurity, CAVs may communicate over VANET. In the future, more CAV data and computation will be moved to the cloud. Although the cloud would then become a central point of target for the adversaries, the target is by no means an easy one. More effort will be required by adversaries to breach an infrastructure that is managed by a consortium of companies and governments. Additionally, security knowledge and intelligence in the cloud can be used to inform CAVs security.

In summary, these countermeasures require no modifications of the GPS signal, the satellite infrastructure, or the GPS receiver. Moreover, they are resistant to a wide range of attack types and might be deployed using multiple standard GPS receivers. Understanding the vulnerabilities of countermeasures themselves can be used to further ensure against attack.

Public safety, consumer privacy, and attack prevention depend upon proper consideration of the cybersecurity and safety threats that CAVs jamming and spoofing attacks pose.

V. CONCLUSION AND FUTURE WORK

The development of autonomous vehicle technology is growing with rapid pace. However, the security aspect of vehicle is not receiving deserved attention, and this gap might prove a serious threat to CAVs security and adoption as many countries are trying to bring autonomous vehicles on road soon. CAV researchers are increasingly giving priority to and collaborating to ensure adequate cybersecurity at design, development, and deployment stages. Accurate and valid sensor, GPS, and cloud-based data are critical for safe and appropriate driving decisions of all kinds. This paper discussed attacks to which the CAV navigation is vulnerable. It also addressed countermeasures to mitigate these attacks. As the automotive domain is strongly cost-driven, the proposed countermeasures are mostly applicable in software. The paper also addressed limitations of these countermeasures.

This paper aims to cover most of the common cyber-attacks and exploits that are possible on CAVs. This is most dynamic area and the attacks are getting sophisticated day by day and aggression are always finding new way sand tools to deceive and hack the vehicle.

This is a most critical area of cybersecurity, and it will prove dynamic as new countermeasures are developed to neutralize and thwart increasingly sophisticated forms of attack. Keeping security considerations in mind in early design phases, and well during development and development of CAVs is critical both to public safety and the success of the CAVs industry.

REFERENCE

[1] R. Dhanasingaraja, S. Kalaimagal, G. Muralidharan, “Autonomous vehicle navigation and mapping system,” Division of Mechatronics, Madras Institute of Technology, Anna University, Chennai, India.

[2] S. Parkinson, P. Ward, K. Wilson, and J. Miller, “Cyber threats facing autonomous and connected vehicles: Future challenges,” IEEE Transactions on Intelligent Transportation Systems, vol. 18, no. 11, pp. 2898–2915, 2017.

[3] Wen, Hengqing, Huang, Peter Yih-Ru, Dyer, John, Archinal, Andy, Fagan, John, "Countermeasures for GPS Signal Spoofing," Proceedings of the 18th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2005), Long Beach, CA, September 2005, pp. 1285-1290.

[4] J. Larcom, H. Liu (2013). “Modeling and characterization of GPS spoofing.” 2013 IEEE International Conference on Technologies for Homeland Security (HST). doi:10.1109/ths.2013.6699094

[5] Tippenhauer, N. O., Pöpper, C., Rasmussen, K. B., &Capkun, S. (2011). “On the requirements for successful GPS spoofing attacks.” Proceedings of the 18th ACM Conference on Computer and Communications Security - CCS 11. doi:10.1145/2046707.2046719

[6] GPS.gov, "What is GPS?," National coordination office for space-based positioning, navigation, and timing, 17 January 2013. [Online]. Available: www.gps.gov/systems/gps/.

[7] P. Bolourchi&S.Uysal (2013). “Forest fire detection in wireless sensor network using fuzzy logic;” Proceedings of the 2013 Fifth International Conference on Computational Intelligence, Communication Systems and Networks; Madrid, Spain. 5–7 June 2013; pp. 83–87.

[8] N. Ziraknejad, P.D. Lawrence, & P.D. Romilly(2015) “Vehicle occupant head position quantification using an array of capacitive proximity sensors.” IEEE Trans. Veh. Technol. 2015; 64:2274–2287. doi: 10.1109/TVT.2014.2344026.

[9] Automotive sensors and electronics expo. [(accessed on 11 October 2017)]; Available online: http://www.automotivesensors2017.com.

[10] W.J. Fleming, New automotive sensors—A review. IEEE Sens. J. 2008; 8:1900–1921. Doi: 10.1109/JSEN.2008.2006452. [CrossRef]

[11] S. Abdelhami, H.S. Hassanein H.S., & G Takahara (2014) “Vehicle as a mobile sensor.” Procedia Comput. Sci. 2014; 34:286–295. doi: 10.1016/j.procs.2014.07.025.

[12] N.S. Yeshodara, N.S. Nagojappa, & N. Kishore (2014). “Cloud based self-driving cars.” 2014 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM). doi:10.1109/ccem.2014.7015485

[13] J. Guerrero-Ibáñez, S. Zeadally, & J. Contreras-Castillo (2018). “Sensor technologies for intelligent transportation systems.” Sensors, 18(4), 1212. doi:10.3390/s18041212

[14] F. Rosique, P.J. Navarro, C. Fernández, & A. Padilla (2019). “A systematic review of perception system and simulators for autonomous vehicles research.” Sensors, 19(3), 648.doi:10.3390/s19030648

[15] K. C. Zeng, S. Liu, Y. Shu, D. Wang, H. Li, Y. Dou, G. Wang, and Y. Yang. (2018). “All your GPS are belong to us: Towards stealthy manipulation of road navigation systems.” In USENIX Security 18, pages 1527–1544, Baltimore, MD. USENIX Association.

[16] P. G. Parakkal& V.V. Sajith Variyar (2017). “GPS based navigation system for autonomous car.” 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI). doi:10.1109/icacci.2017.8126120

[17] T. Nighswander, B. Ledvina, J. Diamond, R. Brumley, & D. Brumley (2012). “GPS software attacks.” Proceedings of the 2012 ACM Conference on Computer and Communications Security - CCS 12. doi:10.1145/2382196.2382245

[18] F. Hoflinger, J. Muller, M. Tork, L. Reindl, & W. Burgard (2012). “A wireless micro inertial measurement unit (IMU).”

2012 IEEE International Instrumentation and Measurement Technology Conference Proceedings. doi:10.1109/i2mtc.2012.6229271

[19] B. G. Stottelaar. (Feb. 2015). "Practical cyber-attacks on autonomous vehicles." [Online]. Available: http://essay.utwente.nl/66766/

[20] C. Yan (2016). Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle.

[21] J.Torchinsky (2016) "Hackers show that tesla autonomous sensors can be fooled, but it's all a bit stupid" (Aug. 4, 2016, 1:50 pm), Jalopnik.com, http://jalopnik.com/hackers-show-that-tesla-autonomoussensors-can-be-foole-1784825823 (last visited Nov. 19, 2016).

[22] S.Taha& X. Shen (2013). "Secure IP mobility management for VANET. dordrecht: springer.

[23] Glushko Technology Law & Policy Clinic (TLPC) . (2016). "Jamming and spoofing attacks: Physical layer cybersecurity threats to autonomous vehicle systems." [Online]. Available: https://tlpc.colorado.edu/wp-content/uploads/2016/11/2016.11.21-Autonomous-Vehicle-Jamming-and-Spoofing-Comment-Final.pdf

[24] V.L.L Thing & J. Wu (2016). "Autonomous vehicle security: a taxonomy of attacks and defences." 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). doi:10.1109/ithings-greencom-cpscom-smartdata.2016.52

[25] D. Dmitri et al, "Path planning for autonomous vehicles in unknown semi-structured environments," Int. J. Robot. Res., vol. 29, no. 5, pp. 485–501, 2010.

[26] J. Levinson et al, "Towards fully autonomous driving: Systems and algorithms," in Proc. Intell. Veh. Symp. (IV), 2011.

[27] X previously 34

[28] P. Y.Montgomery, T. E.Humphreys, & B.M. Ledvina "Receiver-autonomous spoofing detection: Experimental results of a multiantenna receiver defense against a portable civil GPS spoofer." In ION ITM (2009).

[29] H.-Y. Cheng, B.-S. Jeng, P.-T. Tseng, and K.-C. Fan, "Lane detection with moving vehicles in the traffic scenes," IEEE Transactions on intelligent transportation systems, vol. 7, no. 4, pp. 571–582, 2006.

[30] S. Eum and H. G. Jung, "Enhancing light blob detection for intelligent headlight control using lane detection," IEEE Transactions on Intelligent Transportation Systems, vol. 14, no. 2, pp. 1003–1011, 2013.

[31] J. Petit, B. Stottelaar, & M. Feiri (2015) "Remote attacks on automated vehicles sensors: Experiments on camera and LiDAR".

[32] J. Khan (2017) "Vehicle network security testing," in: 2017 Third International Conference on Sensing, Signal Processing and Security (ICSSS), 2017, pp. 119–123. doi:10.1109/SSPS.2017.8071577.

[33] Goldberg, Z. (2016, November 21). "Autonomous Vehicle Cybersecurity Threats: Physical Layer Jamming and Spoofing Attacks." Retrieved from https://tlpc.colorado.edu/autonomous-vehicle-cybersecurity-threats-physical-layer-jamming-and-spoofing-attacks/

[34] M.G. KUHN (2004) An asymmetric security mechanism for navigation signals. In Information Hiding.

[35] K.D Wesson, D.P. Shepard, J.A. Bhatti, J. A., & T.E Humphreys. "An evaluation of the vestigial signal defense for civil GPS anti-spoofing. In ION GNSS" (2011).

[36] Volvo Car City Safety w/Collision Warning. [(accessed on 27 March 2018)]; Available online:http://volvo.custhelp.com/app/answers/detail/a_id/9766/~/city-safety-w%2Fcollision-warning

★★★