A survey on driverless vehicles: from their diffusion to security features

Fabio Arena*, Giovanni Pau, and Mario Collotta
Kore University of Enna, Enna, Italy
{fabio.arena, giovanni.pau, mario.collotta}@unikore.it

Abstract

This paper focuses on state of the art concerning autonomous driving vehicles (AV), with particular attention to standard equipment currently in use and future improvements. The development of these vehicles will allow achieving better safety standards, less environmental pollution, and greater social equity. The development of appropriate infrastructures is not the only requirement that can make all this possible. Therefore, it is necessary to identify the main characteristics that tomorrow's smart cities must hold to accommodate the new technologies introduced by the AV. In this paper, the ranking of the top 20 countries in the world ready to welcome these technologies is analyzed. Another essential feature that is investigated concerns to the security of AVs' dissemination. In particular, all the possible risk factors regarding security, which currently limits the diffusion of this technology, are also analyzed.

Keywords: driverless vehicles, autonomous vehicles, security

1 Introduction

Autonomous Vehicles (AVs), also known as driverless vehicles, are cars or trucks that operate without human drivers, using a combination of sensors and software for navigation and control. An increasing number of partially self-contained vehicles are already on roads and use technologies such as parking assistance and lane change warning. These and other technologies are evolving rapidly. The rapid development of AVs is explained by the high interest shown by private developers and public authorities. Many companies, including major automotive manufacturers, technology giants, and startuppers have invested $50 billion in this market sector over the past five years to develop new AV technologies, with 70% of spending from outside industry investors automotive [58]. Public authorities also notice the enormous potential in the AVs, both in economic terms and regarding social benefits. AVs could eliminate 90% of road accidents caused by human error, saving up to a million lives each year. Electric motors can also power these vehicles with the aim to reduce road pollution and also to improve the quality of life of citizens. AVs offer mobility benefits for people who are not currently able to drive, including the elderly, those who do not own a car and those who live in rural areas that do not have adequate public transport. A study estimates that the US economy could witness an increase of 1.3 trillion dollars a year thanks to the spread of AVs. For these reasons and beyond, many national governments are keen to adopt the AVs as soon as possible massively. Here are some aids supplied with these vehicles that allow them to operate independently:

- Radar: emits sound waves that bounce on objects around the car and its path. The radar can work in all weather conditions and can calculate the speed and distance of objects but can not differentiate between them.

Journal of Internet Services and Information Security (JISIS), volume: 8, number: 3 (August 2018), pp. 1-19
*Corresponding author: Faculty of Engineering and Architecture, Kore University of Enna, Cittadella Universitaria, 94100 Enna, Italy, Tel: +39-0935-536494

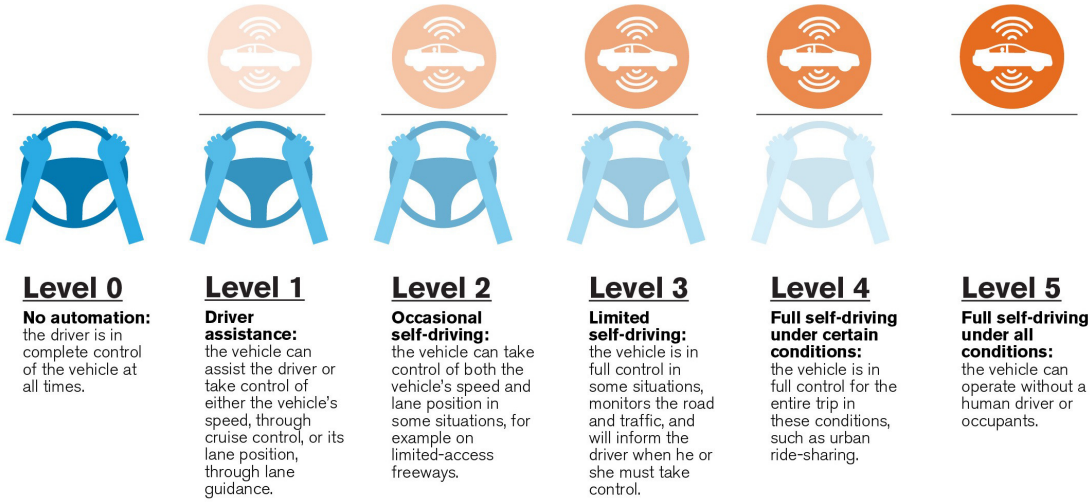

Figure 1: Autonomy levels of a vehicle.

- Laser Scanner: also called LiDAR system (Light Detection and Ranging), emits light pulses that reflect objects to generate a three-dimensional map of the surrounding environment. It can work in the dark by recognizing the horizontal signs on the road.

- Video camera: detects objects in front of the car as traffic lights, pedestrians, cyclists or other cars and works with a vehicle onboard computer.

- Onboard computer: manages real-time inputs from the camera, radar, and laser scanner and combines them with mapping and navigation data to control vehicle operation.

- Network functionalities: ”connected” cars can communicate directly with other vehicles and/or infrastructures, such as new generation traffic lights.

A significant difficulty to be faced in the development of driverless vehicles concerns the skills of the passenger [48]. In fact, should it be only transported or could it decide from time to time? As every commuter knows, everyday driving is often dull and being a mere passenger can be even more so. Now, let’s imagine combining the worst of both situations: the driver’s need to concentrate on slow traffic while being a mere passenger most of the time. In the USA, the National Highway Traffic Safety Administration (NHTSA) and the SAE (Society of Automotive Engineers) use a six-level classification scheme (shown in Figure 1) to indicate the autonomy of a vehicle [63]:

- *Level 0* represents a vehicle in which there are no particular automations, and any decision is left to the driver of the vehicle.

- *Level 1* includes primary driving assistance systems such as the adaptive cruise control system, representing the first level in the scale of autonomous vehicles.

- *Level 2* allows a real driving autonomy with constant driver control (like the automatic pilot on the cars produced by Tesla).

- *Level 3* allows the driver to divert attention to certain types of roads safely but requires him to be ready to take over again if necessary.

It is the next step in the evolution of autonomous commercial cars. Audi is ready to launch a level 3 car by 2018. Other major automakers, including Nissan, Honda, and Kia, will follow. However, Ford threw new doubts on the wisdom of this progression, discovering during the level 3 system tests that drivers lose "situational awareness," sometimes even falling asleep. This situation makes them unable to take over quickly if necessary. The problem persists even after the addition of buzzers, vibrating seats, and a second driver to observe that in the driver's seat [25]. However, by 2021, it is planned to build completely autonomous cars without pedals and steering wheel. The intent is to create a suitable vehicle for the sharing of the journey or the passage on board, presumably within a limited and predefined area: well-mapped city streets, for instance. This situation is the level 4 autonomy. Level 5 represents an entirely autonomous system: vehicles must behave in all respects at least as human drivers and therefore be able to go anywhere, in every imaginable condition and be able to face the most unpredictable situations. This means traveling on dirt roads outside the maps, in storms, thunderstorms or pitch dark, with animals peeking out of bushes, children chasing balls in the street and drivers doing crazy things. Level 5 cars and trucks will have to do all this and more to perform this role.

In this paper, an overview of the infrastructure of AVs and the problems that need to be addressed with some urgency is carried out. Moreover, the security challenges of the different technologies integrated into self-driving vehicles, as well as the possible countermeasures to solve them, are investigated.

This paper is organized as follows. Section 2 presents the issues that must be overcome before the large-scale spread of the AVs. Section 3 introduces the system model of driverless vehicles concerning the infrastructure planning, also presenting the growing interest that AVs have gained and the ranking of countries ready for then. In Section 4 ad deep analysis concerning security is carried out and, finally, Section 5 concludes the paper.

2 Open Issues

In literature, there are many works related to AVs. Most of them propose some improvements to be addressed with the aim to make these products more appealing to people. However, five issues must be resolved before autonomously driven cars can massively furrow the roads:

- *higher performance and redundant software* that can be robust even to possible hacker attacks.
- *more advanced and capillary maps*. To date, self-driving cars from Google seem to run smoothly on the roads of Mountain View, California [28]. This situation occurs because the company has essentially created a sort of virtual map of the city (using Google Street View). However, the AVs, with their sensors and their equipment, may not be able to operate freely without such a detailed map of the rest of the world, although to date Google has mapped most of the roads around the globe.
- *more efficient and precise sensors*. Human brains do a masterful job of classifying and reacting to the risks that may arise while driving a vehicle, but the current state of the art of commercially available sensors is not able to process such data so quickly.
- *better Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications*. Once driverless cars start to proliferate, they will need a highly evolved way to communicate with other vehicles on the road. These cars will have to adapt flexibly, re-determining a command on the fly and communicating with other cars without a driver. Currently, the communication between AVs is minimal, and many developments and insights are needed.
- then, there are the so-called *"ethical questions."* Sometimes, a driver must decide whether to turn right or left, for instance, injuring three people in a truck or potentially killing a person on a

motorcycle. These types of ethical dilemmas would require appropriate software in driverless vehicles that can weigh all the different possible cases, reaching a final solution autonomously. A vehicle capable of doing this would have no precedents in human history. Even remote-controlled vehicles or drones that target the warring enemies are crewed by a human who has the last "word" on the choices to make. There is always a human on the other side who must make a decision. Driverless cars may have to choose who survives in an accident. Recent research conducted in Italy [7] tried to answer this question, making sure that the control and responsibility of the actions of a machine were returned to the driver. The research team has designed a quadrant that allows changing the setting of a car from "altruism" to "selfish" via a convenient intermediate setting. The car would then use the settings chosen by the owner to calculate the actions to be performed, taking into consideration the likelihood that passengers or other parties will suffer damage as a result of the car decision [66]. It is too early to decide whether this will be a good solution but indeed welcomes a vision within a strongly thorny debate [10].

3 System Model of Driverless Vehicles

3.1 Infrastructure Planning

The world is one step away from an essential revolution in the transport sector. Technology is transforming this area, and the pace of innovation is accelerating more and more. Already, in the coming years, it will change not only the way we travel but also the way we will live. It will be revolutionized the way companies import materials, distribute their products, and employ staff. Electric vehicles, mobility on demand, digital railways, deliveries by drones, and very high-speed trains are just some of the components of this revolution. However, the real breakthrough is represented by autonomous driving vehicles which will truly transform our lives. It will mean, for the first time in history, that freedom of mobility will be available to everyone and anywhere. Many people believe that several years will pass before we see entirely autonomous vehicles on our roads; it is probably right. Nevertheless, almost everyone recognizes the potential benefits introduced by autonomously driven vehicles.

There will be economic benefits because the time we currently spend driving a car will become available time that can be spent working, relaxing or sleeping. Besides, there will be social benefits including a significant reduction (about 1.3 million each year) of the number of people killed in traffic accidents, as well as accessibility to transportation even for those who currently can not drive due to age or disability. However, the challenges to be faced are several and as well as the questions to be solved. Will the AVs increase congestion? Will they be used for criminal purposes? What public transport systems will we need in the future? The dimension of this global opportunity and the awareness that the authorities around the world are grappling with these questions have become a source of inspiration for the preparation of this paper which seeks to show also the state of the art of technologies and infrastructures in the major countries of the world. The various countries are compared, and a score is evaluated which will eventually determine a ranking that will allow hypothesizing some conclusions.

The question is no longer whether, but when all the road vehicles will become completely autonomous. This time could be 10 or 30 years then it is clear how many are the implications and how much they can influence the choices of all national governments. These will have to start (or perhaps they should have already done so) to plan the future development of the AVs now. However, why take action now rather than wait to see how quickly the AVs can be developed? A key reason why governments need to consider AVs now is that the investment decisions on land and infrastructure planning we are taking today will determine the development of our countries and cities for decades. If we foresee a future in which the AV can travel, today it will be possible to avoid wasting taxpayers' money on investments that could soon prove obsolete or, worse, frustrate the realization and development of the

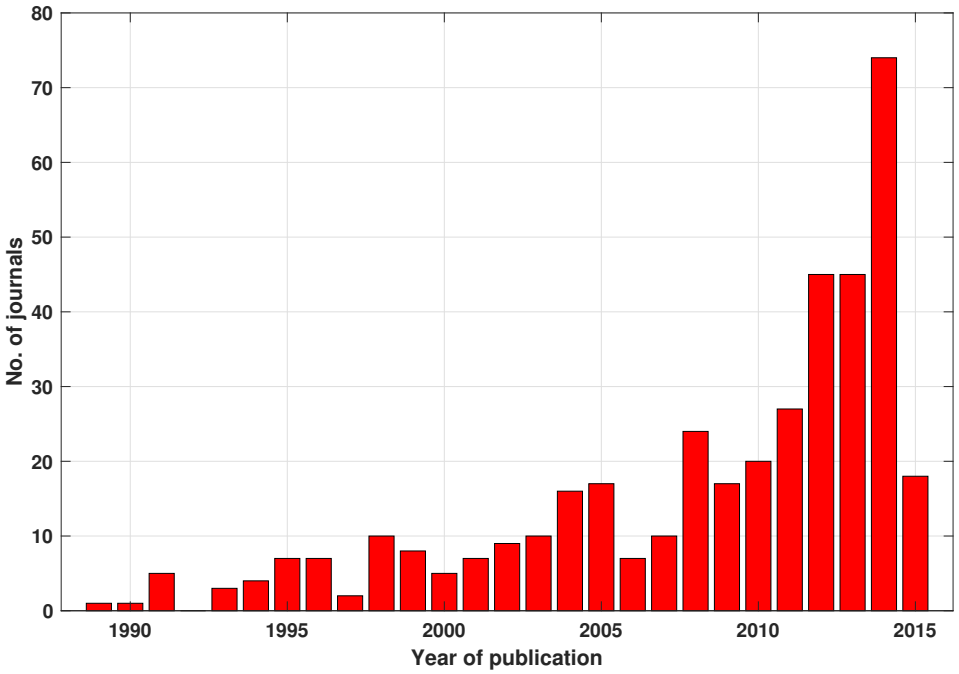

Figure 2: Analysis of publications over time.

AV.

The implications and changes necessary for road infrastructure are numerous and require extensive planning; indeed, we should expect to realize an information acquisition system based on a network of roadside sensors or other sources, able to collect notifications and then exchange and share them. The technology can be used in all phases of the life of the infrastructure and driving experience: info-mobility systems, sensors, instruments to detect the status of bridges, viaducts, and tunnels, as well as vehicle-infrastructure connection technologies, determining for the development of the AVs. Therefore, real telematic roads, appropriate signage, road barriers, adequate widths of lanes and curbs will be necessary.

Public transport planning will also influence integration with AVs, as well as new parking facilities and multi-modal ticket issuing systems. The AV will also influence the positioning and development of homes and businesses. In fact, the so-called "phenomena" of shared mobility of a journey could represent a very engaging paradigm. This situation would determine the possible use of the space currently utilized for public parking to be able to build civil homes and/or public spaces in urban areas.

The AVs will also determine other essential impacts on public policy, outside transport in the strict sense. For instance, many taxi drivers may be at risk of being replaced by technology. On the other hand, it could increase the new employment in the automotive sector, in the supply chain industries, and in the road maintenance industries. Significant and severe implications for the revenue of national governments could also arise. So far, for instance, fossil fuel taxes generate billions of dollars in public revenues while electric vehicles receive subsidies in many countries. This occurrence means that a switch to electric AVs would create a hole in the public coffers. The authorities will, therefore, have to think how to recover these lost revenues urgently. For example, through road pricing that would also minimize and counter possible congestion phenomena.

The future development of the AVs certainly implies several other initiatives that must be undertaken to safeguard public safety. The authorities will have to make sure that the AVs are safe both from a me-

chanical point of view and regarding security from cyber attacks (new data security control systems will have to be implemented). The regulation of road traffic, currently designed to be used by human beings, will have to be replaced by protocols that will determine priorities at intersections, leaving appropriate free spaces for emergency vehicles. In general, therefore, it is clear that different countries of the world will come to different conclusions but, at the base, the standards of interoperability must be implemented in their respective nations and potentially also between the various continents. So now it is time to plan, as long as it is not too late.

3.2 The Growing Interest to AVs

In Figure 2, it is possible to evaluate the development of self-driving cars research throughout the last decades (until 2015). It is highlighted, at the same time, a continuous increase of the interest on the topic, as well as essential milestones that can also influence the development and research [47]. It is useful to note the case of the DARPA Grand Challenges at the beginning of 2004 and end of 2005 or the Urban Challenge at the end of 2007 (DARPA, 2015), that were relatively crucial events in the field. Furthermore, from 2013 to 2014, a rapid increase of 60.8% can be observed, which can be related to the actual interest in the topic. In addition to the points already analyzed, it would be necessary to deepen and improve four fundamental features to make the development of AV in the various countries of the world as simple as possible: policy and legislation, technology and innovation, infrastructures and consumer acceptance [28].

3.3 Ranking of Countries Ready for AVs

The analysis carried out in this research paper is based on four specific aspects that are crucial for the development of autonomous vehicles. In particular they specifically concern:

- national policy and legislation;
- technology and innovation;
- existing and future infrastructures;
- the interest shown by consumers of these vehicles.

On the basis of the analysis of the scores assigned to these four parameters, a real ranking (shown in Table 1) has been drawn up that will allow us to establish which countries in the world are currently more predisposed to welcome the new technologies introduced by the AV in the best possible way [28].

4 Security in Driverless Vehicles

As shown in [5], the terrorist attacks perpetrated by driving commercial and non-commercial vehicles into large crowds between July 2016 and August 2017 have resulted in more than 100 fatalities and many more injuries. These attacks have affected many communities around the globe including Barcelona in Spain, London in England, Stockholm in Sweden, Berlin in Germany, Ohio in the US, and Nice in France. In most cases, it has only taken a single driver to attack with such devastating consequences, which affected not only the immediate victims but also the overall community psyche.

These data may be one of the many motivations in the development and adoption of self-driving vehicles due to their potential of increasing road safety, transportation safety, and preventing the abuse of vehicles as mass murder weapons. However, findings from surveys undertaken in the U.S., the U.K., and Australia showed that 67.8% of the respondents expressed moderate to high concerns in self-driving

Table 1: Ranking of top 20 countries worldwide regarding capacity to accept the AVs.

Overall rank	Country	Total score	Policy and legislation		Technology and innovation		Infrastructure		Consumer acceptance	
			Rank	*Score*	*Rank*	*Score*	*Rank*	*Score*	*Rank*	*Score*
1	The Netherlands	27.73	3	7.89	4	5.46	1	7.89	2	6.49
2	Singapore	26.08	1	8.49	8	4.26	2	6.72	1	6.63
3	United States	24.75	10	6.38	1	6.97	7	5.84	4	5.56
4	Sweden	24.73	8	6.83	2	6.44	6	6.04	6	5.41
5	United Kingdom	23.99	4	7.55	5	5.28	10	5.31	3	5.84
6	Germany	22.74	5	7.33	3	6.15	12	5.17	12	4.09
7	Canada	22.61	7	7.12	6	4.97	11	5.22	7	5.30
8	United Arab Emirates	20.89	6	7.26	14	2.71	5	6.12	8	4.79
9	New Zeland	20.75	2	7.92	12	3.26	16	4.14	5	5.43
10	South Korea	20.71	14	5.78	9	4.24	4	6.32	11	4.38
11	Japan	20.28	12	5.93	7	4.79	3	6.55	16	3.01
12	Austria	20.00	9	6.73	11	3.69	8	5.66	13	3.91
13	France	19.44	13	5.92	10	4.03	13	4.94	10	4.55
14	Australia	19.40	11	6.01	13	3.18	9	5.43	9	4.78
15	Spain	14.58	15	4.95	16	2.21	14	4.69	17	2.72
16	China	13.94	16	4.38	15	2.25	15	4.18	15	3.13
17	Brazil	7.17	20	0.93	18	0.86	19	1.89	14	3.49
18	Russia	7.09	17	2.58	20	0.52	20	1.64	18	2.35
19	Mexico	6.51	19	1.16	17	1.01	17	2.34	19	2.00
20	India	6.14	18	1.41	19	0.54	18	2.28	20	1.91

vehicle's security, 68.7% of the respondents showed the same level of concern in the system's security, and 63.7% of the respondents showed the same level of concern in regards to their data privacy [49]. Thus, it is not surprising that the research community has started examining and addressing potential security issues and vulnerabilities present in the different components of self-driving vehicles.

Technologies enabling self-driving vehicles can be divided into Autonomous Vehicle and Cooperative Intelligent Transport Systems (C-ITS) (Europe), also known as Connected Vehicle Technologies (USA) [39]. C-ITS and Connected Vehicle Technologies largely depend on Vehicular Ad-Hoc Networks (VANETs) for transmitting Cooperative Awareness Messages in C-ITS or Basic Security Messages in Connected Vehicles Technologies [55]. On the other hand, Autonomous Vehicles often combine different technologies to achieve the desired autonomy level. As an example, the authors of [74] combined a Light Detection and Ranging system (LiDAR) with Stereo Cameras to detect surrounding vehicles. Additionally, the authors of [12] propose to use novel methods, such as deep learning and the tensor flow framework, to navigate a driverless vehicle. Nevertheless, none of the developed technologies have been able to reach full-autonomy as a standalone product.

The concept presented in Figure 3 is motivated by Loukas and Patrikakis [11], where they identified the components of the Internet of Everything and decomposed its threats. We reorganized and adapted this concept based on the structure of self-driving vehicles concerning identifying individual security elements and their corresponding threats (Figure 3). Furthermore, we classify these elements into cyber and physical groups where our interest is to identify the means and impact when seeking to attack a target vehicle. We also classify the different technologies equipped in self-driving vehicles into four categories, as follows:

1. Sensing Technologies: LiDAR, VLC, Ultrasonic Ranging Devices (URD), Millimeter Wave Radar, and Infrared Ranging.

2. Positioning Technologies: GPS and Radars (Doppler Radar Speedometers, Radar Cruise Control, and Radar Based Obstacle Detection Systems).

3. Vision Technologies: HD Cameras, Stereo Vision Systems, and CCTVs.

4. Vehicular Networks: VANET's, Automotive Ethernet, Byteflight, Controller Area Network (CAN), FlexRay, Local Interconnect Network (LIN), Low-Voltage Differential Signaling (LVDS), and Media Oriented Systems Transport (MOST) technologies.

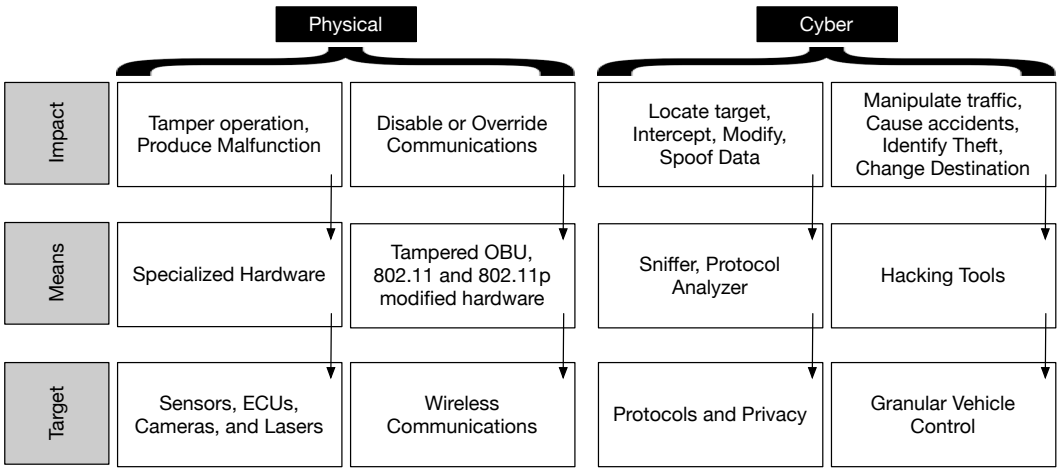

Figure 3: Decomposition of self-driving vehicles' security elements.

Researchers such as Reger [46] suggest manufacturers adopt a security-by-design and privacy-by-design approach in the development of autonomous vehicles. These approaches include isolating different system devices by functionality to different networks, providing regular updates through a 15 years' time span, implementing defense-in-depth security architecture, as well as securing interfaces, communication channels, in-vehicle networks, and ECUs by adopting IT cryptographic technologies, IDS, IPS, firmware updates and virtualization technologies into the automotive industry. All of the previously mentioned approaches, according to Reger [46], shall be considered for adoption while simultaneously providing the highest standards and automotive quality and reliability.

4.1 Vehicles Sensing Technologies

Light Detection and Ranging (LiDAR) is composed of a scanner, a specialized GPS, and a laser to provide remote sensing using pulses of light. These pulses are used to measure distances to generate 3D information of a particular landscape, which can become very precise when combined with airborne system data. Two types of LiDAR technologies have been developed, i.e., topographic LiDAR used to map land using infrared (IR) lasers and bathymetric LiDAR for underwater measurements using green light [38]. Multiple LiDAR systems that have been equipped in vehicles include the Laseroptrnix's LiDAR user by Volvo [75], the ALASCA XT [4], a four-beam LiDAR developed by IBEO, used by Volkswagen and BMW, and the HDL-64E [64] composed of a 64 detector array developed by Velodyne.

The authors of [9] describe how LiDAR systems can be tampered with resulting in health hazards and damaging surveillance systems. The authors depict three scenarios in which eye-safe laser emitters are replaced with a hazardous green/IR laser inside the turret housing and change the device's objective from recognizing its surroundings to point the laser beam to an intended target aided by the IR camera. In the first scenario, the turret is placed above a vehicle which sets it at a height in range to that of an average person [62] in the U.S. The laser beams are helped with computer vision and trained machine learning models for face recognition. They can be targeted to a person's eyes in order to cause ocular harm which might not be recognized as such by the affected victim as stated in [23]. The second scenario examines the same setting as in scenario one during nighttime in which case the pupils are more dilated, and the laser can cause more harm. The third scenario is focused on recognizing and damaging camera systems using a green laser emitter.

Presented countermeasures include those introduced in [61]. In this case, the authors propose the use of windshield-laminated glass to act as a UV filter, combining glass with plastic polyvinyl butyral

to be used as a passive low pass filter, using IR rejection filters to function as a bandpass filter, and protective lenses for cameras that will obscure when an attacker aims beams at the camera and trigger an image capture to determine the culprit. Since pedestrian protection is more difficult, the authors suggest building tamper-proof sensor array housings and distinctive features on OEM parts to prevent housing falsifications and make tampering elements detectable during inspections.

Petit and Shaldover [39] present the potential cyber threats to automated vehicles as well as the proof-of-concept on LiDAR attacks. On the contrary, the authors of [8] express how Petit tricked the LiDAR system by making it detect a false obstacle in front of it, which can be interpreted as a false pedestrian or vehicle, with the use of a Raspberry PI and a laser pointer. The Raspberry I is coupled with a laser pointer to which it sends pulses. The beam was pointed towards the self-driven vehicle equipping a LiDAR at a distance of 100m. The LiDAR was tricked and represented illusory objects as physical objects taking the vehicle to a complete stop. The author of [50] expresses that a misbehavior detection system correlated with other data inputs have the potential to mitigate the risk of this attack.

4.2 Vehicles Positioning Technologies

Global Positioning System (GPS) receivers are one of the most used technologies at present day with a noticeable integration within personal vehicles, smartphones, aviation vehicles, watches, fitness trackers, and space vehicles. Two types of attacks can be devised in GPS receivers, these being GPS Jamming and GPS Spoofing. The former involves an attacker interfering with the GPS bands (L1 at 1575.42 MHz and L2 at 1227.60 MHz) while the latter is more complicated in the sense that GPS spoofing involves modifying position, velocity, and time (PVT) values; an example of such a case is presented in [3] where the attack effects extend to the VANET.

Spoofing techniques include pseudo-random noise (PRN) code phase and carrier phase adjustment to match the phases on the target's signals [29]. Effective countermeasures include those based on Receiver Autonomous Integrity Monitoring (RAIM) or spatial processing methods; although, the usage of an antenna array results in an increased complexity [36] [34].

Warner and Johnston [21] demonstrated the ease in spoofing GPS signals by using a GPS satellite simulator. The simulator is used to broadcast a fake GPS signal with a strength higher than an original GPS signal and provide the receiver with an incorrect position and/or time information. Additionally, the authors presented seven countermeasures to detect suspicious signal activity: monitoring the absolute GPS signal strength, monitoring the relative GPS signal strength, monitoring the signal strength of each received satellite signal, monitoring the satellite identification codes and the number of satellite signals received, checking the time intervals, performing a time comparison, and performing a sanity check.

Nils et al. [59] examined the minimum precision required of an attacker's spoofing signals to perform GPS spoofing attacks and the practical aspects of a satellite lock takeover. Using civilian GPS generators, the authors performed a series of experiments where they focused on the relative signal power of the spoofing signal, the constant time offset influence, the location offset influence, and the relative time offsets influence to validate the effects of spoofing signals under different scenarios. Their findings indicate that the attacker must ensure that his time offset to the target system is less than 75ns, which corresponds to a distance of 22.5m from the target. Besides, they found that the initial location offset performed during the attack would cause a jump in the victim's reported position. Thus, these parameters need to be taken into account by the victim in order to detect and prevent such attacks. As a countermeasure, the authors suggested the use of multiple GPS receivers where these receivers will exchange their location. The GPS receiver can then check over time if a new calculated location preserves their initial estimated physical formation. Under a spoofing attack, their saved (or last known) physical location will pass pre-defined certain error bounds.

Kerns et al. [24] presented their conclusions on the conditions necessary to successfully perform a

spoofing attack in an unmanned aerial vehicle (UAV) and the required range of the attack. The authors concluded that the spoofer is required to have an estimation error of the UAV position and velocity below 50m and 10m/s in order to succeed with a cover to capture the target receiver's tracking loops. Additionally, they explored their capability to produce a post-capture control authority over a target UAV and showed that a GPS spoofing attack could force a UAV to follow a path defined by the attacker without the target's awareness.

Psiaki et al. [42] proposed a method to inform a defender receiver if tracked publicly known GNSS signals are reliable or not when an attacker attempts to spoof signals for multiple satellites with the objective of overlaying original signals. In successful attacks, the attacker can slowly divert the target away from the correct time and location in a self-aware manner. RAIM is unable to detect such attacks since it only looks for signal inconsistencies during navigation. The authors' technique tracks the publicly known signal in a secure reference receiver and a defender receiver; additionally, the signal tracking data is used to isolate its encrypted part. Before cross-correlating encrypted signals, the PRN code of the encrypted signal is required; the encrypted parts isolated from the two receivers are cross-correlated. If a high cross-correlation statistic is detected, then it is an indication that no spoofing is detected. On the other hand, a low cross-correlation statistic will indicate that spoofing was detected.

Other methods for detecting GPS spoofing include: detecting changes on power and time-related parameters, value analysis at correlator output, spatial processing, implementation of cryptographic algorithms, usage of hybrid navigation systems (GNSS+INS) as proposed by Jwo et al. in [22], the evidence accrual system presented by Stubberud and Kramer in [56][57], and the VANET assisted V2I communication for GPS spoofing detection presented by [2]. Furthermore, a performance assessment on the previously stated mitigation methods is presented by Magiera, and Katulski [33], GPS spoofing tests against phasor measurement units (PMUs) are presented by [53], and approaches for restoring operation of spoofed GPS receivers can be found in [20]. GPS receiver can be complemented with Doppler radar speedometers, radar cruise control, and radar-based obstacle detection systems, some of the consumer products are available for integration in self-driving vehicles to deliver additional active location validation.

4.3 Vehicles Vision Technologies

Vision systems ranging from CCTV to Stereo Vision have been critical components due to their capability of providing visual information. Regardless of how this information is computed at its destination, the provision of confidentiality, integrity, and authenticity of such data is critical to determine further actions. Although several encryption proposals have been published for a variety of applications with available high computational capabilities, very few can be adapted for low computational capability systems.

Gonçalves and Costa [13] list the symmetric and asymmetric cryptography algorithms used in image encryption as well as their advantages and disadvantages. Symmetric encryption algorithms such as AES, DES, and IDEA utilize a single key for encryption and decryption functionality, and while the implementation of such algorithms relatively does not have high computational overhead, the real challenge is focused on securely distributing the shared key. On the other hand, asymmetric encryption algorithms such as Rabin's scheme, RSA, and ECC use a private key for decryption and a public key for encryption. In such algorithms, distribution of public key is feasible, but the computational overhead is high although ECC provides a greater implementation in environments requiring smaller keys (such as wireless communications) since it requires smaller encrypted messages in comparison with RSA [44].

Authors also present image security solutions applicable in scenarios under processing power and energy supply constraints. Selective Image Encryption as presented by Sadourny and Conan [51], Pfarrhofer and Uhl [40], and Liu [32] provide an image security solution with less computational overhead and a reasonable security level. This goal is achieved by encrypting only a section of the compressed data

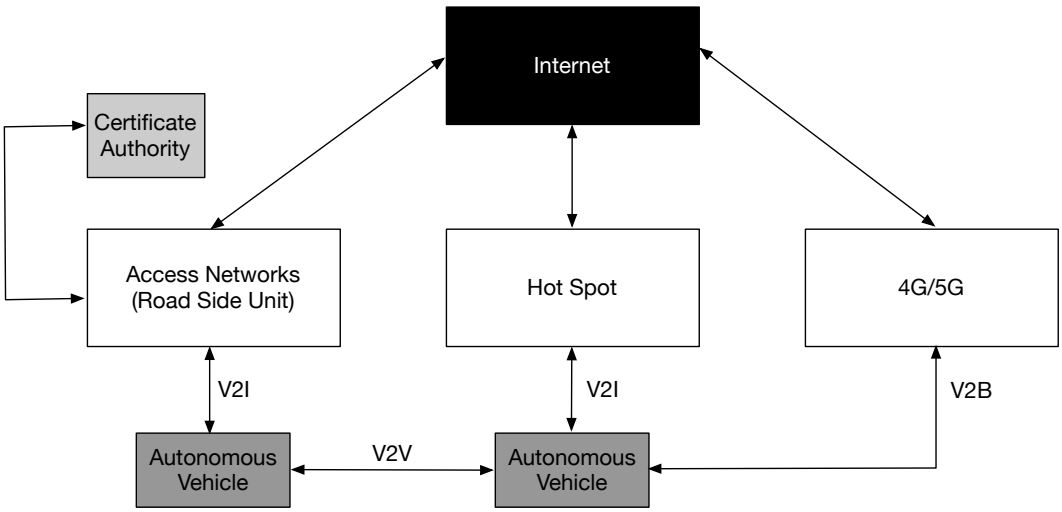

Figure 4: VANET reference architecture adapted from [30] and [45].

using encryption algorithms with higher efficiency than the ones used in traditional encryption [41]. Coding algorithms suited for selective image encryption include Quadtree-Based Image coding and Wavelet coding. Quadtree is an attractive compression algorithm due to its low complexity and can use either lossy or lossless coding [37].

On the other hand, Wavelet-Based Image coding uses pyramid decomposition, and its algorithms are based on zero-trees permitting to insignificant group coefficients within these trees as well as defining the coefficient's importance by level. At the highest compression level, root level, we will find the most relevant visual information. Also, a discrete wavelet transform algorithm is used in order to determine the data sets to be partitioned. Selective encryption mechanisms for video and image transmitted through wireless sensor networks include Wang et al. UEP-Based approach [69] and Xiang et al. DWT-Based approach [71].

In systems incapable of procession cryptographic algorithms, watermarking can be utilized in order to provide possible authentication mechanisms and detect video forgery. Digital watermarks can be embedded into image and video data in order to provide a means to verify ownership of such data to the receiver. These digital watermarks are embedded within the initially transmitted data, they hide authentication information, and can either be visible or not. An example with such a solution is presented by Harjito et al. in [16] where the group covers the generation, embedding, and detection of watermarks; additionally, Harito et al. also explore the implementation of their solution over wireless sensor networks in [17]. Due to the nature of how watermarking is embedded within data, their solution introduces new challenges dependent on the original data type; as an example, scalar data. Solutions for watermarking used in scalar data are presented by Shi and Xiao [54] and Xiao et al. in [72]. Watermarking used in multimedia transmitted over wireless sensor networks is introduced by Harjito et al. in [15]. Discrete Cosine Transform (DCT) coding to embed watermarks is explored by Yu et al. in [73]. An approach where watermarks are embedded optimally and adaptively to improve error resiliency by carefully allocating network resources for watermarked images is presented by Wang [67]. Limitations of using an active video forgery detection mechanism such as watermarking include the systems inability to prevent the owner from manipulating video and the use of specialized hardware for post-processing.

4.4 Vehicles Networks

Vehicular Ad-Hoc Network (VANET) is an emergent technology capable of enhancing driving safety, traffic efficiency, and accident reduction by transmitting information between vehicles and the surrounding infrastructure through different communication types such as vehicle-to-vehicle (V2V) communication and vehicle-to-infrastructure (V2I). To achieve the aforementioned, technologies such as IEEE 802.11p were developed to meet with ITS applications requirements. While different aspects of VANETs are being researched, there is a broad interest to start the deployment of this technology in the nearby future. Sjoberg et al. [55] present a staged VANET deployment strategy which is divided into four phases. Phase 1, awareness driving, enables vehicles to become aware of each other and inform about road hazards. Phase 2, sensing driving, enables vehicles to provide information captured by sensors equipped in the vehicle and use this information to have accurate knowledge of their surroundings. Phase 3, cooperative driving, permits vehicles to share intended future actions with other vehicles such as destinations and maneuvers. Phase 4, synchronized cooperative driving - Accident-Free Driving, refers to vehicles capable of driving autonomously under any scenario, synchronizing trajectories and accomplishing optimal driving patterns.

VANET's use different type of communication protocols depending on the communication type. In Figure 4, an overview of the architecture in VANETs is shown. As it can be observed, onboard units are a crucial component to autonomous vehicles due to their ability to enable vehicle-to-everything (V2X) type of communications. Onboard devices, such as the ones developed by Savari [52], provide connectivity to the vehicle's controller access network (CAN) through which it can obtain information from the ECUs on different components.

Mishra et al. [35] present the most prominent communication technologies in VANET including IEEE 802.16, also known as WiMAX, which delivers a 30 mile communication range, and 802.11p which is utilized for Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) operating at a 5.9 GHz, a frequency licensed by Intelligent-Transport-Systems (ITS). Some of the prerequisites that need to be provided by a security system include authentication, reliability, integrity, anonymity, availability, delay handling, and confidentiality. The transmission of messages in VANETs are critical for offering its users with a wide range of features and applications to enable the improvement of road safety. Nevertheless, the secure transmission of such messages depends on the different components used within the network and their resiliency to different attacks. In order to prevent existing vulnerabilities from being exploited, several security components are set in place within the system's architecture. These security components include authentication, anonymity, availability, confidentiality, delay handling, integrity, and reliability. Mishra et al. [35] break down the VANET attack types into network attacks, application attacks, timing attacks, social attacks, and monitoring attacks.

5 Conclusions

Research and experimentation in the automotive area are an essential element in the development of AVs. Three of the first five countries of the present study have significant capacities to this effect. However, this aspect alone is not enough, as can be seen from the third place in the United States. While the U.S. is a global leader for innovation, they have a joint assessment of legislation and do not make the most of existing infrastructure. Sweden and Germany, in second and third place for technology and innovation, have gaps in other aspects of development [28].

Road transport is mainly based on the quality of highway infrastructure and on the regulatory environment that determines access to these infrastructures. Excellent performance in both these areas gives Singapore, the second highest rating in the index despite a less impressive rating on the technology. The limited attention paid to infrastructure undermines the ambitions of the United Kingdom, Canada, and

New Zealand. The Netherlands is leading this index because it has a strong performance in all four pillars of research, showing how both the private and public sectors are very committed to achieving this goal [28]. Electric vehicles are already ubiquitous, and even the existing infrastructures appear to be excellent and ready to welcome the new technologies introduced by the AV. So what would it take to accelerate the application of AVs technologies in several countries? From this research and the opinions of stakeholders all over the world, at least three areas of particular interest must be facilitated and promoted:

1. plan the future and development of the AVs today, reviewing current national and local transport strategies, as well as expected investment development projects. Support the introduction and the diffusion of electric vehicles through measures that allow also increasing the recharge points. Investing in high-quality road infrastructure and next-generation mobile communications (for instance, V2V, V2I technologies).

2. introduce specific legislation aimed at removing possible regulatory obstacles, as well as the promotion of a dedicated national body within the government, which promotes the adoption of the AVs and contributes to financing innovation. This goal could help to speed up the development of technologies and ensure their application to the demands and objectives that the public requires.

3. promote synergies and partnerships between public authorities and private sector developers, like Singapore, in particular. Gathering all critical stakeholders around a table to discuss how to overcome the emerging problems in the deployment of self-driving vehicles. In this sense, it should be recognized that it is not just urban or extra-urban transport, but how citizens think of developing communities of tomorrow, where they live and where will work.

Several nations of the world are now focusing on driverless technologies. Among these, the United States certainly plays a predominant role. On the contrary, in Europe, the United Kingdom and the Netherlands are also stimulating research in this area. However, it is clear that the real breakthrough will have to be carried out by car manufacturers. Most of them plan to test the market with autonomous vehicles of level 3 or possibly level 4 around 2021. Such AVs will still have steering wheels and pedals and be able to drive autonomously only on pre-established roads. Most of these vehicles are likely to be purchased from onboard transit services (for instance, Uber and others).

Consumers who want the flexibility and freedom of complete level 5 vehicles will have to wait for some time. The major car manufacturers (Tesla, General Motors, Ford, Fiat-Chrysler, Waymo to name a few of the main ones) like to talk about autonomous vehicles as if they will be on sale in their showrooms in three or four years. The pleasant situation that the producers present, however, could come true one day. However, it is unlikely that this day is still so close.

The number of driverless vehicles globally is likely to increase in the foreseeable future, and this is likely to create not only a more significant potential target for malicious users but also a potentially more substantial number of adverse incidents relating to the exploitation of vulnerabilities contained in the vehicles. In this paper, the range of attacks and security concerns that can affect the different technologies that underpinned self-driving vehicles (Figure 5) have been reviewed and discussed. For instance, it has been shown that LiDAR systems could either be the target of the attack or become the source of the attack by modifying embedded lasers. The capabilities of VLC have also been explored and, as a result, the attacks on this technology must be executed through a LOS based on the literature available.

It has been examined how GPS spoofing could be performed, and described mitigation strategies, and functionality restoration proposals. Besides, radar-based systems, capable of complimenting GPS functionality, have been presented. It has also been examined the stereo vision systems as well as security methods utilized in other vision technologies that could be implemented on them. Security methods

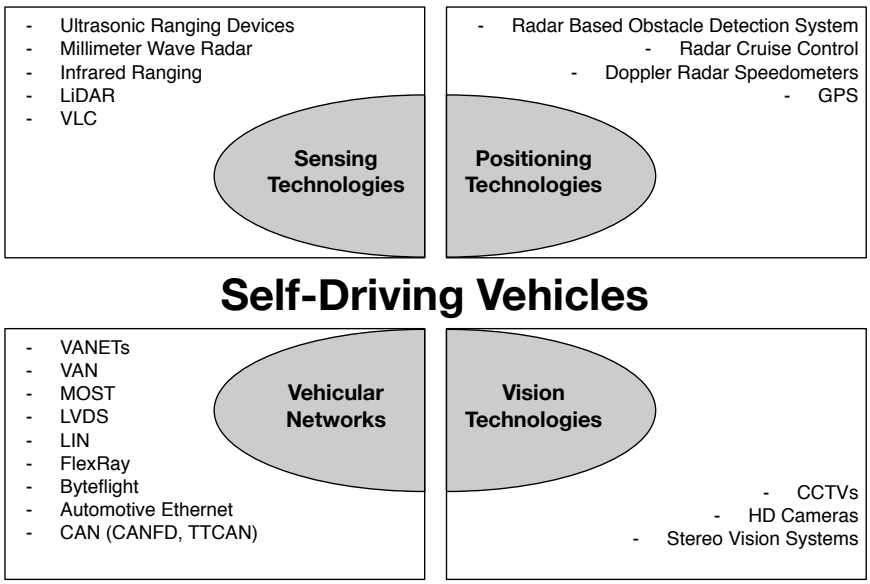

Figure 5: Technologies equipped in self-driving vehicles.

included active video forgery detection using watermarking as well as passive video forgery detection. The discussion of vehicle networks focused on VANETs and In-Vehicle Networks. In VANETS, it has been presented the challenges on these networks as well as the different range of attacks classified by attack vector that can be performed within the VANET. Also, an in-depth explanation of the different mitigation strategies has been presented. For in-vehicle networks, the different networking technologies that have been equipped with different vehicle models have been shown.

Moreover, existing capability differences and the range of applications each can cover have been analyzed. Based on the obtained results, different security solutions that can be implemented for each technology and found literature supporting such statements have been exhibited. Then, the different technologies that can be equipped with self-driving vehicles to enable them to reach the desired autonomy level [60] have been summarized.

Generally, efforts have been devoted to addressing security and privacy concerns present in driverless vehicles, although future attempts should be more holistic and coordinated. However, cyber protections are seldom absolute. As stated in [14], "*When a security incident occurs, we may need to conduct an investigation to establish the root cause of the incident and how it could be prevented in the future.*" In other words, forensic investigators and incident responders will likely need to rely on the residual data from vehicles affected by the incident and potentially the underpinning technologies. Internet of Things and vehicle forensics are relatively new [6, 19, 70], in comparison to the other branches of digital forensics such as hard disk forensics, network forensics and cloud forensics (cloud security is also another widely studied area [68, 65, 27, 26]). Unless the vehicles and the underpinning technologies have built-in forensic collection facilities, data required in a forensic investigation may not always be available. Hence, we posit the need to extend the forensic-by-design principle coined in [14, 1, 43] to the development of future driverless vehicles. This feature also echoes the observations of Huang, Lu and Choo [18] and Lin et al. [31] who recently noted the importance of having forensically ready/friendly vehicular fog computing systems and the Internet of Drones.

References

[1] N. H. Ab Rahman, N. D. W. Cahyani, and K.-K. R. Choo. Cloud incident handling and forensic-by-design: cloud storage as a case study. *Concurrency and Computation: Practice and Experience*, 29(14):e3868, May 2016.

[2] B. Anouar, B. Mohammed, G. Abderrahim, and B. Mohammed. Vehicular navigation spoofing detection based on v2i calibration. In *Proc. of the 2016 4th IEEE International Colloquium on Information Science and Technology (CiSt'16), Tangier, Morocco*, pages 847–849. IEEE, October 2016.

[3] S. Bittl, A. A. Gonzalez, M. Myrtus, H. Beckmann, S. Sailer, and B. Eissfeller. Emerging attacks on vanet security based on gps time spoofing. In *Proc. of the 2015 IEEE Conference on Communications and Network Security (CNS'15), Florence, Italy*, pages 344–352. IEEE, September 2015.

[4] C. Boehlau and J. Hipp. Optoelectric sensing device with common deflection device. `https://www.google.com/patents/US7345271` [Online; accessed on July 15, 2018], 2017.

[5] CNN. Terrorist Attacks by Vehicle Fast Facts. `http://www.cnn.com/2017/05/03/world/terrorist-attacks-by-vehicle-fastfacts/index.html` [Online; accessed on July 15, 2018], 2017.

[6] M. Conti, A. Dehghantanha, K. Franke, and S. Watson. Internet of things security and forensics: Challenges and opportunities. *Future Generation Computer Systems*, 78(Part 2):544–546, January 2018.

[7] G. Contissa, F. Lagioia, and G. Sartor. The ethical knob: ethically-customisable automated vehicles and the law. *Artificial Intelligence and Law*, 25(3):365–378, September 2017.

[8] M. H. Eiza and Q. Ni. Driving with sharks: Rethinking connected vehicles with vehicle cybersecurity. *IEEE Vehicular Technology Magazine*, 12(2):45–51, June 2017.

[9] R. Felix, J. Economou, and K. Knowles. Driverless vehicles and lidar: Evaluation of possible security threats on the open road. Technical Report 2015-01-0219, SAE International, April 2015.

[10] E. Frazzoli, M. A. Dahleh, and E. Feron. Real-time motion planning for agile autonomous vehicles. In *Proc. of the 2001 American Control Conference (ACC'01), Arlington, Virginia, USA*, volume 1, pages 43–49. IEEE, June 2001.

[11] G. Loukas and C. Patrikakis. Cyber and physical threats to the Internet of Everything. *Cutter IT Journal*, 29(7):5–11, July 2016.

[12] N. Gallardo, N. Gamez, P. Rad, and M. Jamshidi. Autonomous decision making for a driver-less car. In *Proc. of the 12th System of Systems Engineering Conference (SoSE'17), Waikoloa, Hawaii, USA*, pages 1–6. IEEE, June 2017.

[13] D. d. O. Gosalves and D. G. Costa. A survey of image security in wireless sensor networks. *Journal of Imaging*, 1(1):4–30, June 2015.

[14] G. Grispos, W. B. Glisson, and K. R. Choo. Medical cyber-physical systems development: A forensics-driven approach. In *Proc. of the 2017 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE'17), Philadelphia, Pennsylvania, USA*, pages 108–113. IEEE, July 2017.

[15] B. Harjito, S. Han, V. Potdar, E. Chang, and M. Xie. Secure communication in wireless multimedia sensor networks using watermarking. In *Proc. of the 4th IEEE International Conference on Digital Ecosystems and Technologies (DEST'10), Dubai, United Arab Emirates*, pages 640–645. IEEE, April 2010.

[16] B. Harjito, V. Potdar, and J. Singh. Watermarking technique for wireless multimedia sensor networks: A state of the art. In *Proc. of the 2012 CUBE International Information Technology Conference (CUBE'12), Pune, India*, pages 832–840. ACM, September 2012.

[17] B. Harjito, V. Potdar, and J. Singh. Watermarking technique for wireless sensor networks: A state of the art. In *Proc. of the 8th International Conference on Semantics, Knowledge and Grids (SKG'12), Beijing, China*, pages 253–256. IEEE, October 2012.

[18] C. Huang, R. Lu, and K. R. Choo. Vehicular fog computing: Architecture, use case, and security and forensic challenges. *IEEE Communications Magazine*, 55(11):105–111, November 2017.

[19] D. Jacobs, K. R. Choo, M. Kechadi, and N. Le-Khac. Volkswagen car entertainment system forensics. In *Proc. of the 2017 IEEE Trustcom/BigDataSE/ICESS, Sydney, New South Wales, Australia*, pages 699–705. IEEE, August 2017.

[20] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle. Gps vulnerability to spoofing threats and a review of antispoofing techniques. *International Journal of Navigation and Observation*, 2012:1–16, May 2012.

[21] J.S. Warner and R.G. Johnston. GPS Spoofing Countermeasures. *Homeland Security Journal*, LAUR-03-6163:19 – 27, January 2003.

[22] D. Jwo, F. Chung, and K. Yu. Gps/ins integration accuracy enhancement using the interacting multiple model nonlinear filters. *Journal of Applied Research and Technology*, 11(4):496 – 509, August 2013.

[23] A. M. Kelley, J. MacDonnell, D. Grigley, J. Campbell, and S. J. Gaydos. Reported back pain in army aircrew in relation to airframe, gender, age, and experience. *Aerospace Medicine and Human Performance*, 88(2):96–103, February 2017.

[24] A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys. Unmanned aircraft capture and control via gps spoofing. *Journal of Field Robotics*, 31(4):617–636, April 2014.

[25] A. M. Khan, A. Bacchus, and S. Erwin. Policy challenges of increasing automation in driving. *IATSS Research*, 35(2):79 – 89, March 2012.

[26] A. Khoshkbarforoushha, A. Khosravian, and R. Ranjan. Elasticity management of streaming data analytics flows on clouds. *Journal of Computer and System Sciences*, 89:24–40, November 2017.

[27] A. Khoshkbarforoushha, R. Ranjan, R. Gaire, E. Abbasnejad, L. Wang, and A. Y. Zomaya. Distribution based workload modelling of continuous queries in clouds. *IEEE Transactions on Emerging Topics in Computing*, 5(1):120–133, January 2017.

[28] KPMG. Autonomous-vehicle-readiness-index. `http://www.home.kpmg.com` [Online; accessed on July 15, 2018], 2018.

[29] B. M. B. Ledvina, W. J., B. Galusha, and I. Miller. An in-line anti-spoofing device for legacy civil gps receivers. In *Proc. of the 2010 International Technical Meeting of The Institute of Navigation (ION GNSS'09), San Diego, California, USA*, pages 698–712. ION, January 2010.

[30] W. Liang, Z. Li, H. Zhang, S. Wang, and R. Bie. Vehicular ad hoc networks: Architectures, research issues, methodologies, challenges, and trends. *International Journal of Distributed Sensor Networks*, 11(8):745303, August 2015.

[31] C. Lin, D. He, N. Kumar, K. R. Choo, A. Vinel, and X. Huang. Security and privacy for the internet of drones: Challenges and solutions. *IEEE Communications Magazine*, 56(1):64–69, January 2018.

[32] J.-L. Liu. Efficient selective encryption for jpeg 2000 images using private initial table. *Pattern Recognition*, 39(8):1509 – 1517, August 2006.

[33] J. Magiera and R. Katulski. Detection and mitigation of gps spoofing based on antenna array processing. *Journal of Applied Research and Technology*, 13(1):45 – 57, February 2015.

[34] M. Meurer, A. Konovaltsev, M. Cuntz, and C. Hattich. Robust joint multi-antenna spoofing detection and attitude estimation using direction assisted multiple hypotheses raim. In *Proc. of the 25th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS'12)*, pages 3007–3016. ION, September 2012.

[35] R. Mishra, A. Singh, and R. Kumar. Vanet security: Issues, challenges and solutions. In *Proc. of the 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT'16), Chennai, India*, pages 1050–1055. IEEE, March 2016.

[36] Montgomery, P.Y. and T.E. Humphreys and B.M. Ledvina. A Multi-Antenna Defense Receiver-Autonomous GPS Spoofing Detection. In *Proc. of the 22nd International Technical Meeting of the Satellite Division of Institute of Navigation (ION GNSS'09), Savannah, Georgia, USA*. ION, March 2009.

[37] S. K. Naveenkumar, H. T. Panduranga, and Kiran. Partial image encryption for smart camera. In *Proc. of the 2013 International Conference on Recent Trends in Information Technology (ICRTIT'13), Chennai, India*, pages 126–132. IEEE, July 2013.

[38] N.O. and A.A. US Department of Commerce. What is LIDAR. `http://oceanservice.noaa.gov/facts/lidar.html` [Online; accessed on July 15, 2018], 2017.

[39] J. Petit and S. E. Shladover. Potential cyberattacks on automated vehicles. *IEEE Transactions on Intelligent Transportation Systems*, 16(2):546–556, April 2015.

[40] R. Pfarrhofer and A. Uhl. Selective image encryption using jbig. In *Proc. of the 2005 IFIP International Conference on Communications and Multimedia Security (CMS'05), Salzburg, Austria*, volume 3677 of *Lecture Notes in Computer Science*. Springer, Berlin, Heidelberg, September 2005.

[41] M. Podesser, H. peter Schmidt, and A. Uhl. Selective bitplane encryption for secure transmission of image data in mobile environments. In *Proc. of the 5th Nordic Signal Processing Symposium (NORSIG'02), Trondheim, Norway*, page 1037, October 2002.

[42] M. L. Psiaki, B. W. O'Hanlon, J. A. Bhatti, D. P. Shepard, and T. E. Humphreys. Gps spoofing detection via dual-receiver correlation of military signals. *IEEE Transactions on Aerospace and Electronic Systems*, 49(4):2250–2267, OCTOBER 2013.

[43] N. H. A. Rahman, W. B. Glisson, Y. Yang, and K. R. Choo. Forensic-by-design framework for cyber-physical cloud systems. *IEEE Cloud Computing*, 3(1):50–59, January 2016.

[44] G. V. S. Raju and R. Akbani. Elliptic curve cryptosystem and its applications. In *Proc. of the 2003 IEEE International Conference on Systems, Man and Cybernetics. Conference Theme - System Security and Assurance (SMC'03), Washington, D.C., USA*, pages 1540–1543. IEEE, October 2003.

[45] M. Raya, P. Papadimitratos, and J. Hubaux. Securing vehicular communications. *IEEE Wireless Communications*, 13(5):8–15, October 2006.

[46] L. Reger. 1.4 the road ahead for securely-connected cars. In *Proc. of the 2016 IEEE International Solid-State Circuits Conference (ISSCC'16), San Francisco, California, USA*, pages 29–33. IEEE, January 2016.

[47] Rosenzweig, J. and Bartl, M. A Review and Analysis of Literature on Autonomous Driving. The Making of Innovation, E-Journal, October 2015.

[48] P. E. Ross. Robot, you can drive my car. *IEEE Spectrum*, 51(6):60–90, June 2014.

[49] S. Brandon and M. Sivak. A Survey of Public Opinion About Autonomous and Self-Driving Vehicles in the U.S., the U.K., and Australia. `https://deepblue.lib.umich.edu/bitstream/handle/2027.42/108384/103024.pdf?sequence=1&isAllowed=y` [Online; accessed on July 15, 2018], July 2017.

[50] S. Curtis. Self-driving cars can be hacked using a laser pointer. `http://www.telegraph.co.uk/technology/news/11850373/Self-driving-carscan-be-hacked-using-a-laser-pointer.html` [Online; accessed on July 15, 2018], 2017.

[51] Y. Sadourny and V. Conan. A proposal for supporting selective encryption in jpsec. *IEEE Transactions on Consumer Electronics*, 49(4):846–849, November 2003.

[52] Savari. MobiWAVE: On-Board-Unit (OBU). `http://savari.net/technology/on-board-unit/` [Online; accessed on July 15, 2018], 2018.

[53] D. P. Shepard, T. E. Humphreys, and A. A. Fansler. Evaluation of the vulnerability of phasor measurement units to gps spoofing attacks. *International Journal of Critical Infrastructure Protection*, 5(3):146 – 153, December 2012.

[54] X. Shi and D. Xiao. A reversible watermarking authentication scheme for wireless sensor networks. *Information Sciences*, 240:173 – 183, August 2013.

[55] K. Sjoberg, P. Andres, T. Buburuzan, and A. Brakemeier. Cooperative intelligent transport systems in europe: Current deployment status and outlook. *IEEE Vehicular Technology Magazine*, 12(2):89–97, June 2017.

[56] S. C. Stubberud and K. A. Kramer. Analysis of fuzzy evidence accrual security approach to gps systems. In *Proc. of the 2014 10th International Conference on Communications (COMM'14), Bucharest, Romania*, pages 1–6. IEEE, May 2014.

[57] S. C. Stubberud and K. A. Kramer. Threat assessment for gps navigation. In *Proc. of the 2014 IEEE International Symposium on Innovations in Intelligent Systems and Applications (INISTA'14), Alberobello, Italy*, pages 287–292. IEEE, June 2014.

[58] Telematica Trasporti e Sicurezza. Il Mercato dei Sistemi Intelligenti di Trasporto in Italia: quadro attuale e prospettive (in Italian) - Available at: http://www.ttsitalia.it. `http://www.ttsitalia.it` [Online; accessed on July 15, 2018], 2018.

[59] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Capkun. On the requirements for successful gps spoofing attacks. In *Proc. of the 18th ACM Conference on Computer and Communications Security (CCS'11), Chicago, Illinois, USA*, pages 75–86. ACM, October 2011.

[60] G. Torre, P. Rad, and K.-K. R. Choo. Driverless vehicle security: Challenges and future research opportunities. *Future Generation Computer Systems*, January 2018.

[61] C. Tuchinda, S. Srivannaboon, and H. W. Lim. Photoprotection by window glass, automobile glass, and sunglasses. *Journal of the American Academy of Dermatology*, 54(5):845–854, May 2006.

[62] U.S. Census Bureau. Cumulative Percent Distribution of Population by Height and Sex: 2007 to 2008. `http://www.cdc.gov/nchs/nhanes.htm` [Online; accessed on July 15, 2018], 2012.

[63] US Department of Transportation (NHTSA). Automated Driving Systems: a Vision for Safety 2.0 - Technical report. `https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf` [Online; accessed on July 15, 2018], 2017.

[64] Velodyne. LiDAR HDL-64E S3 High Definition LiDAR Sensor. `https://velodynelidar.com/lidar/products/manual/HDL-64E%20S3%20manual.pdf` [Online; accessed on July 15, 2018], 2013.

[65] M. Villari, M. Fazio, S. Dustdar, O. Rana, and R. Ranjan. Osmotic computing: A new paradigm for edge/-cloud integration. *IEEE Cloud Computing*, 3(6):76–83, November 2016.

[66] S. L. Vine, A. Zolfaghari, and J. Polak. Autonomous cars: The tension between occupant experience and intersection capacity. *Transportation Research Part C: Emerging Technologies*, 52:1–14, March 2015.

[67] H. Wang. Communication-resource-aware adaptive watermarking for multimedia authentication in wireless multimedia sensor networks. *The Journal of Supercomputing*, 64(3):883–897, June 2013.

[68] L. Wang, Y. Ma, A. Y. Zomaya, R. Ranjan, and D. Chen. A parallel file system with application-aware data layout policies for massive remote sensing image processing in digital earth. *IEEE Transactions on Parallel and Distributed Systems*, 26(6):1497–1508, June 2015.

[69] W. Wang, M. Hempel, D. Peng, H. Wang, H. Sharif, and H. Chen. On energy efficient encryption for video streaming in wireless sensor networks. *IEEE Transactions on Multimedia*, 12(5):417–426, August 2010.

[70] S. Watson and A. Dehghantanha. Digital forensics: the missing piece of the internet of things promise. *Computer Fraud and Security*, 2016(6):5–8, June 2016.

[71] T. Xiang, C. Yu, and F. Chen. Fast encryption of jpeg 2000 images in wireless multimedia sensor networks. In *Proc. of the 2013 International Conference on Wireless Algorithms, Systems, and Applications (WASA'13), Zhangjiajie, China*, volume 7992 of *Lecture Notes in Computer Science*, pages 196–205. Springer, Berlin, Heidelberg, 2013.

[72] R. Xiao, X. Sun, and Y. Yang. Copyright protection in wireless sensor networks by watermarking. In *Proc. of the 2008 International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP'08), Harbin, China*, pages 7–10. IEEE, August 2008.

[73] P. Yu, S. Yao, J. Xu, Y. Zhang, and Y. Chang. Copyright protection for digital image in wireless sensor network. In *Proc. of the 2009 5th International Conference on Wireless Communications, Networking and Mobile Computing*, pages 1–4. IEEE, September 2009.

[74] F. Zhang, D. Clarke, and A. Knoll. Vehicle detection based on lidar and camera fusion. In *Proc. of the 17th International IEEE Conference on Intelligent Transportation Systems (ITSC'14), Qingdao, China*, pages 1620–1625. IEEE, October 2014.

[75] M. Zhao, A. Mammeri, and A. Boukerche. Distance measurement system for smart vehicles. In *Proc. of the 7th International Conference on New Technologies, Mobility and Security (NTMS'15), Paris, France*, pages 1–5. IEEE, July 2015.

Author Biography

Fabio Arena received the Bachelor Degree in Telecommunication Engineer from University of Catania in 2006. He also received the Master Degree in Telecommunication Engineering from University of Catania in 2010. Currently, he is a Ph.D. student at Kore University of Enna. His current research interests include ITS, driverless vehicle and network architecture.

Giovanni Pau is a professor at Faculty of Engineering and Architecture, Kore University of Enna, Italy. Prof. Pau received his Bachelor degree in Telematic Engineering from University of Catania, Italy; and his Masters degree (cum Laude) in Telematic Engineering and PhD from Kore University of Enna, Italy. Prof. Pau has published more than 35 papers in journals and conferences and authored 1 book chapter. He serves as Associate Editor of several journals. Moreover, he serves/served as a leading Guest Editor in several special issues. He collaborates/collaborated with the organizing and technical program committees of several conferences in order to prepare conference activities and is serving as a reviewer of several international journals and conferences. His research interests include wireless sensor networks, soft computing techniques, internet of things, home automation and real-time systems.

Mario Collotta received his PhD in 2011 from Catania University, Italy, on the topic of factory automation networks. Since 2010 he has served as an Assistant Professor with tenure in the Faculty of Engineering and Architecture at the Kore University of Enna, Italy, and in 2011 he becomes a principal researcher and director of the Computer Engineering and Network Laboratory. His research interests concern the realization of strategies and innovative algorithms in order to ensure a flexible management of resources in real- time systems and networks. He is a member of the IEEE and has published 2 book chapters, and over 60 refereed international journals and conference papers. He has served on several committees of distinguished journals and international IEEE conferences. He is currently an Associate Editor of some Elsevier and Springer journals. Dr Collotta has also served as a Guest Editor and Lead Guest Editor of several special sections and special issues focused on the study of real-time networks, systems and applications.