Future Generation Computer Systems ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Driverless vehicle security: Challenges and future research opportunities

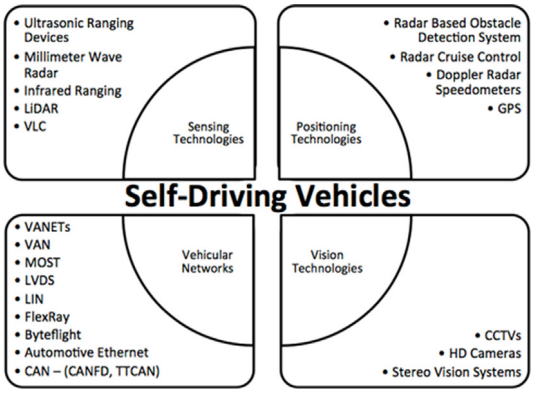
Gonzalo De La Torre [a], Paul Rad [b,a], Kim-Kwang Raymond Choo [b,a,*]

[a] Department of Electrical and Computer Engineering, The University of Texas at San Antonio, San Antonio, TX 78249, United States
[b] Department of Information Systems and Cyber Security, The University of Texas at San Antonio, San Antonio, TX 78249, United States

HIGHLIGHTS

- Driverless vehicle security and privacy challenges.
- Driverless vehicle security and privacy research opportunities.
- Technologies equipped in self-driving vehicles.
- Sensing, positioning, vision, and network technologies in driverless-vehicles.

GRAPHICAL ABSTRACT



ARTICLE INFO

Article history:
Received 7 July 2017
Received in revised form 5 October 2017
Accepted 24 December 2017
Available online xxxx

Keywords:
Self-driving vehicles
Driverless vehicles
Intrusion detection
Network security
Autonomy and trust

ABSTRACT

As self-driving vehicles become increasingly popular, new generations of attackers will seek to exploit vulnerabilities introduced by the technologies that underpin such vehicles for a range of motivations (e.g. curiosity, criminally-motivated, financially-motivated and state-sponsored). For example, vulnerabilities in self-driving vehicles may be exploited to be used in terrorist attacks such as driving into places of mass gatherings (i.e. using driverless vehicles as weapons to cause death or serious bodily injury). This survey presents a categorized summary of security methodologies developed to secure sensing, positioning, vision, and network technologies that can be equipped in driverless-vehicles. These technologies have the potential to benefit their security from tailored machine learning models. Future research opportunities are also identified.

1. Introduction

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 [1]. In most cases it has only taken a single driver to carry out the attack with such devastating consequences, which not only affected the immediate victims but also the overall community psyche. In a different setting, during 2015, there were reportedly 6,296,000 motor vehicle traffic crashes, a large increase from the 6,064,000 reported crashes in 2014. Furthermore, during 2015 a total of 32,166 crashes were reported as fatal; an increase from the 30,056 fatal crashes reported in 2014 [2].

* Corresponding author at: Department of Information Systems and Cyber Security, The University of Texas at San Antonio, San Antonio, TX 78249, United States.
E-mail addresses: gonzalo.delatorreparra@utsa.edu (G. De La Torre), paul.rad@utsa.edu (P. Rad), raymond.choo@fulbrightmail.org (K.-K.R. Choo).

https://doi.org/10.1016/j.future.2017.12.041
0167-739X/

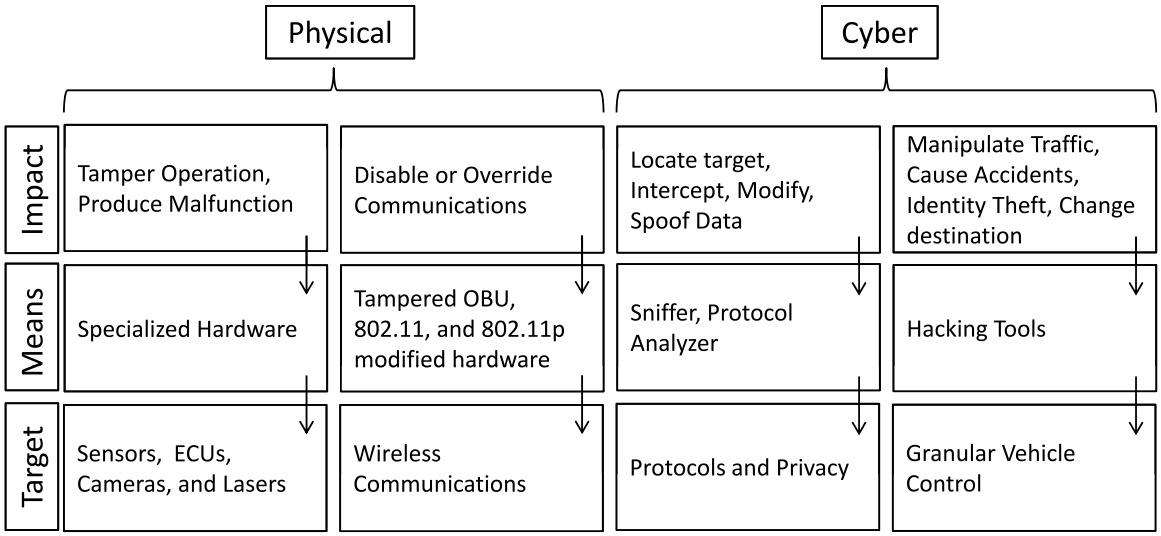


Fig. 1. Decomposition of self-driving vehicles' security elements.

Such statistics 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 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 [3]. 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) [4]. 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 [5]. On the other hand, Autonomous Vehicles often combine different technologies to achieve a desired autonomy level. As an example, Zhang, Clarke, and Knoll [6] combined a Light Detection and Ranging system (LiDAR) with Stereo Cameras to detect surrounding vehicles. Additionally, researchers such as Gallardo et al. [7] 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.

In order to determine how technologically advanced a vehicle is, bill H.R. 3388 SELF DRIVE Act was introduced to the US Congress by Rep. Robert E. Latta. The bill requires the US Department of Transportation to determine the most cost effective method and terminology to inform consumers about the capabilities and limitations of highly automated vehicles [8]. Meanwhile, the National Highway Traffic Safety Administration recently adopted the Society of Automotive Engineers' five levels for automated driving systems [9]. Level 0 refers to a driver in complete control of the vehicle. In Level 1, the vehicle controls specific functions automatically. In Level 2, the vehicle is capable of controlling the steering and acceleration/deceleration motion of the vehicle while obtaining information from the driving environment allowing the driver to disengage from controlling the vehicle. In Level 3, the driver is able to handle control of safety-critical functions to the vehicle and while the driver is able to intervene, it is not required. In Level 4, vehicles are able to control all safety-critical driving functions as well as monitor the driving environment but it is constrained only to a few driving scenarios. Finally, Level 5 refers to fully autonomous systems capable of driving in every scenario and delivering the same level of performance as a human driver. These five levels for automated driving systems should not be confused with the four phases of VANET deployment (i.e. Awareness Driving, Sensing Driving, Cooperative Driving, Synchronized Driving–Accident-Free Driving) [5].

The concept presented in Fig. 1 is inspired by Loukas and Patrikakis [10], where they identify the components of Internet of Everything and decomposed its threats. We reorganized and adapted this concept based on the structure of self-driving vehicles in terms of identifying individual security elements and their corresponding threats (see Fig. 1). 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.

Researchers such as Reger [11] 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,

Please cite this article in press as: G. De La Torre, et al., Driverless vehicle security: Challenges and future research opportunities, Future Generation Computer Systems (2018), https://doi.org/10.1016/j.future.2017.12.041.

according to Reger [11], shall be considered for adoption while simultaneously providing the highest standards and automotive quality and reliability.

In this paper, we will cover the security challenges of the different technologies integrated in self-driving vehicles as well as the possible countermeasures to solve them. The materials presented in this survey were located by searching on ACM Digital Library, IEEE Xplore, ScienceDirect, Springer Link, Google Scholar, Elsevier Journal Finder, and Sage Journals using keywords such as Self-Driving Vehicles Intrusion Detection, Vehicle Security, Vehicle Hacking, Automated Vehicle Security, Automated Vehicle Attacks, VANET Challenges, VANET Security, In-Vehicle Communication Survey, In-Vehicle Networks Security, Vehicle Ranging, LiDAR Security, Visible Light Communication Tampering, GPS Spoofing, Vehicle Radar Security, In-Vehicle Network Security, CCTV Security, Stereo Camera Security, and Video Security. The surveyed literature were published between 1997 and 2017.

Based on our observations of the different technologies that have been gradually integrated into vehicles and their functionality, we categorized our security observations into four main groups, namely: sensing, position, vision, and network technologies.

In Sections 2 and 3, security topics in vehicle sensing technologies (e.g. Light Detection and Ranging — LiDAR, and Visible Light Communication –VLC) and positioning technologies (e.g. GPS) are presented, respectively. In Section 4, vision technologies and the related security solutions are presented. In Section 5, we discuss the security aspects of Vehicular Ad Hoc Networks (VANETs). In Section 6, we present networking technologies adopted by the automotive industry to enable In-Vehicle Communication such as Automotive Ethernet, Automotive Gateway and Vehicle-Wide Network Topology, Byteflight, Controller Area Network (CAN), FlexRay, Local Interconnect Network (LIN), Low-Voltage Differential Signaling (LVDS), and Media Oriented Systems Transport (MOST). Finally, we summarize and describe a potential research agenda in the last section.

In the previously mentioned sections, we take further steps to present not only the technologies to ensure vehicle security but also their vulnerabilities and the potential attacks that can be executed against vehicular components. In addition, we explore the countermeasures to address these security vulnerabilities, attack vectors, and solutions to detect and stop attacks.

2. Vehicle sensing technologies

2.1. Light detection and ranging

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, topographic LiDAR used to map land using infrared (IR) lasers and bathymetric LiDAR for underwater measurements using green light [12].

Multiple LiDAR systems that have been equipped in vehicles include the Laseroptrnix's LiDAR user by Volvo [13], the ALASCA XT [14], a four-beam LiDAR developed by IBEO, used by Volkswagen and BMW, and the HDL-64E [15] composed of a 64 detector array developed by Velodyne.

Felix et al. [16] explain 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 [17] in the US. Helped with computer vision and trained machine learning models for face recognition, the laser beams 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 by Harris et al. [18]. The second scenario contemplates 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 Tuchinda et al. [19] proposing 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 band pass 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 to build tamper proof sensor array housings and distinctive features on OEM parts to prevent housing falsifications and make tampering elements detectable during inspections.

Petit and Shladover [4] present the potential cyber threats to automated vehicles as well as the proof-of-concept on LiDAR attacks. Hashem Eiza and Ni [20] 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 100 m. The LiDAR was tricked and represented illusory objects as physical objects taking the vehicle to a complete stop. Petit [21] expresses that a misbehavior detection system correlated with other data inputs have the potential to mitigate the risk of this attack.

2.2. Visible light communication

Visible Light Communication (VLC) is a technology that has the potential to address problems found using DSRC. This technology is notable for using modulated optical radiation within the visible light spectrum in order to transmit information from one point to another [22]. This technology has been implemented in case studies where data is transmitted between traffic lights and vehicles as presented by Kitano et al. [23] and Kumar [24]; furthermore, the technology has demonstrated to provide stable communication at a range of up to 50 m as presented by Kumar et al. [25], Cailean et al. [26], Cailean et al. [27], Okada et al. [28], and Saito et al. [29]. VLC can be easily integrated with vehicles equipped with LEDs on their front and rear lights and data transition can be achieved by modulating the LEDs amplitude at high frequencies while not affecting its primary lighting function. Some examples where vehicle-to-vehicle (V2V) communication using this technology include Cailean et al. [30], Kim et al. [31], Yoo et al. [32], and Takai et al. [33], where prototypes presented successful communication between vehicles covering a few tens of meters. This technology requires a direct line of sight (LOS) in order to transmit digital information, Jovicic and Richardson [34]. Ucar et al. [22] state that attackers attempting to jam VLC transmitted data between two vehicles would need to direct strong light to jam the target's receivers and while the attack may succeed, the attack success would only be limited to a single VLC link. Pathak et al. [35] also points out that due to the LOS requirement to enable VLC, attackers attempting to launch an attack on the receiving sensors must perform it within the LOS range.

Please cite this article in press as: G. De La Torre, et al., Driverless vehicle security: Challenges and future research opportunities, Future Generation Computer Systems (2018), https://doi.org/10.1016/j.future.2017.12.041.

3. Vehicle location technologies

Global Positioning System (GPS) receivers are one of the most used technologies in our 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 complex in the sense that GPS spoofing involves modifying position, velocity, and time (PVT) values; an example of such a case is presented by Bittl et al. [36] 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 [37]. 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 [38,39].

Warner and Johnston [40] demonstrated the ease in spoofing GPS signals by using a GPS satellite simulator. The simulator is used to broadcast a fake GPS signal with strength greater than an original GPS signal and provide the receiver with an erroneous 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. [41] 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 offset 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 75 ns, which corresponds to a distance of 22.5 m from the target. In addition, 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. [42] presented their findings 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 50 m and 10 m/s in order to succeed with a cover to capture the target receiver's tracking loops. Additionally, they explored their capability to produce a port-capture control authority over a target UAV and showed that a GPS spoofing attack can force a UAV to follow a path defined by the attacker without the target's awareness.

Psiaki et al. [43] proposed a method to inform a defender receiver if its 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 true 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 in a defender receiver; additionally, the signal tracking data is used to isolate its encrypted part. Prior to 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 [44], the evidence accrual system presented by Stubberud and Kramer in [45,46], and the VANET assisted V2I communication for GPS spoofing detection presented by [47].

Furthermore, a performance assessment on the previously stated mitigation methods is presented by Magiera and Katulski in [48], GPS spoofing tests against phasor measurement units (PMUs) are presented by [49], and approaches for restoring operation of spoofed GPS receivers can be found in [50]. GPS receiver can be complimented 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. Vehicle 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 accessible high computational capabilities, very few can be adapted for low computational capability systems. In this section, we present security mechanisms to protect image and video data in systems with low computational capabilities.

4.1. Video and image encryption over wireless sensor networks

Gonçalves and Costa [51] 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 do 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 greater implementation in environments requiring smaller keys (such as wireless communications) since it requires smaller encrypted messages in comparison with RSA [52]. 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 [53], Pfarrhofer and Uhl [54], and Liu [55] provide an image security solution with less computational overhead and a reasonable security level. This is achieved by encrypting only a section of the compressed data using encryption algorithms with higher efficiency than the ones used in traditional encryption [56].

Please cite this article in press as: G. De La Torre, et al., Driverless vehicle security: Challenges and future research opportunities, Future Generation Computer Systems (2018), https://doi.org/10.1016/j.future.2017.12.041.

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 loosy or loosless coding [57]. On the other hand, Wavelet-Based Image coding uses pyramid decomposition and its algorithms are based on zero-trees permitting to group insignificant 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. In addition, 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 [58] and Xiang et al. DWT-Based approach [59].

4.2. Active video forgery detection using watermarking

In systems incapable of procession cryptographic algorithms, watermarking can be utilized in order to provide feasible 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 original 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 [60] where the group covers the generation, embedding, and detection of watermarks; additionally, Harjito et al. also explore the implementation of their solution over wireless sensor networks in [61]. Due to the nature on 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 in [62] and Xiao et al. in [63]. Watermarking used in multimedia transmitted over wireless sensor networks is presented by Harjito et al. in [64]. Discrete Cosine Transform (DCT) coding to embed watermarks is explored by Yu et al. in [65]. 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 [66]. Limitations of using an active video forgery detection mechanism such as watermarking includes the systems inability to prevent the owner from manipulating video and the use of special hardware for post-processing.

4.3. Passive video forgery detection

In contrast with Watermarking, passive video forgery detection focuses on extracted internal video features, which do not require relying on pre-extracted information. Passive video forgery detection mechanisms can be classified into statistical correlation of video features, frame-based for detecting statistical anomalies, and inconsistencies of various digital equipment [67]. Table 1 presents a summary on literature presenting solutions within each one of the stated categories.

4.4. Stereo vision systems

Stereo vision systems apply the principle of observing a scene from two (or more) viewpoints in order to reconstruct a three-dimensional scene using a complementary structured light source. CCD cameras are preferably used due to their low power consumption, low weight, small size, noise resiliency, accurate light measurement, and dynamic range [13]. Stereo vision methods are classified into active and passive methods depending on the resources they utilize to reconstruct a 3D scene. Active stereo methods utilize a complementary structured light source to reconstruct 3D scenes while passive stereo vision methods use the unstructured light sources captured by the camera to reconstruct a 3D scene. Examples of such active methods include Scharstein and Szeliski [79], Couture et al. in [80], and Kerstein et al. in [81].

Automakers are now incorporating stereo vision systems into their models; such an example includes Subaru incorporating their developed product *Eyesight* into various models starting in 2015. Other independent corporations like Bosh are presenting their solutions [82] and publishing their patents [83] based on these technologies.

As presented by Mammeri et al. in [84], stereo vision systems are typically comprised of six modules: image acquisition, camera calibration, feature extraction, stereo matching, 3D reconstruction, and post-processing. It is important to note that video captured by cameras is prone to tampering or modification in the cases where this data travels through an in-vehicle network and attackers have already accessed this system level. In such cases video data can be protected with a variety of techniques as the ones presented in Sections 4.1–4.3. Although these solutions have been used in the past on a variety of different technologies, private companies such as Northrop Grumman have presented patents as in [85] specifically targeting the security of stereo cameras.

5. Vehicle 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 wide interest to start the deployment of this technology in the nearby future. Sjoberg et al. [5] presents 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.

5.1. General architecture

Among the various publications focused on securing autonomous vehicles, various make reference to securing communications on VANETs. VANET's use different type of communication protocols depending on the communication type.

In Fig. 2, we provide an overview of the architecture in VANETs. As it can be observed in Fig. 2, on-board units are a key component to autonomous vehicles due to their ability to enable vehicle-to-everything (V2X) type of communications. On-board devices, such as the ones developed by Savari [86], 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. [89] present the most prominent communication technologies in VANET including IEEE 802.16, also known as WiMAX, which delivers a 30 mile communication range and

Please cite this article in press as: G. De La Torre, et al., Driverless vehicle security: Challenges and future research opportunities, Future Generation Computer Systems (2018), https://doi.org/10.1016/j.future.2017.12.041.

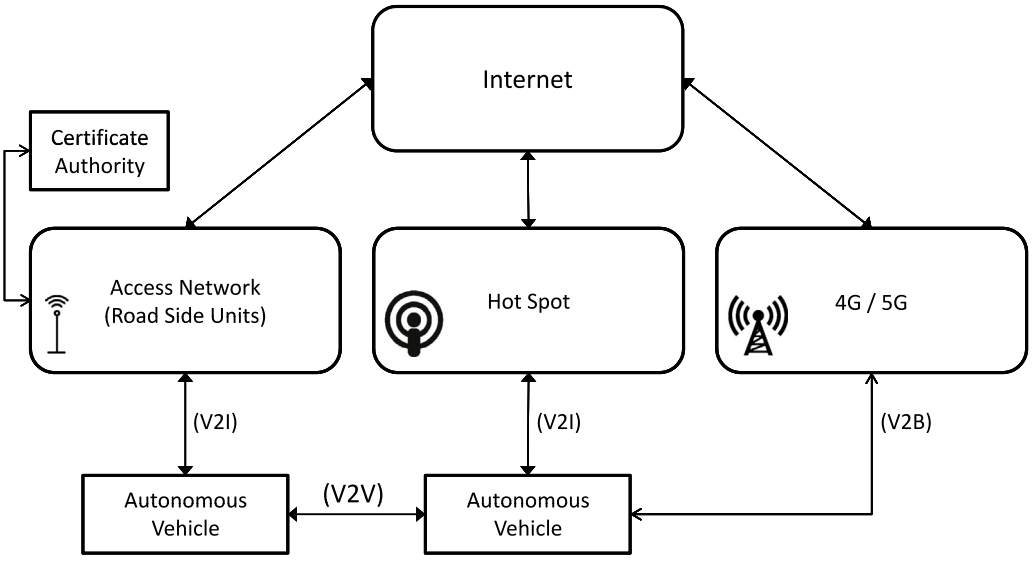


Fig. 2. VANET reference architecture.
Source: adapted from [87] and [88].

Table 1
Summary of passive video forgery detection solutions.
Source: (adapted from [67]).

Category	Forgery addressed	Passive solutions
Statistical correlation of video features	Frame insertion	[68]
	Frame modification	[69]
	Frame insertion	[70]
	Moving object removal	[71]
Frame-based for detecting statistical anomalies	Frame insertion	[72]
	Frame manipulation	
	Frame duplication	[73]
	Region duplication	[74]
	Region duplication in 3D domain	[75]
Inconsistencies of various digital equipment	Inter frame forgery	[76]
	Upscale crop forgery	[77]
	Copy paste	[78]

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.

5.2. Challenges

The deployment of VANETs confronts researchers with many security challenges that can be categorized into technical and socio-economic. Many of these challenges have been discussed by Mishra et al. [89], Vaibhav et al. [90], and Hasrouny et al. [91]. Table 2 provides a summary of challenges identified in the literature.

Authors discussing such challenges include Hartenstein and Laberteaux [92] stating that the main security concerns involve data authenticity where false information can be provided to vehicles, data transmitted through road infrastructure can be modified or vehicles can be impersonated. Networks of trust can reduce the problem by ignoring or distrusting information from certain users.

Mishra et al. [89] identified major security challenges such as consistency of data, high mobility, error tolerance, latency control, and key management. The authors classify the attacks into several categories, these being: attacks based on membership where we can find internal and external attackers, attacks based on the activity where we can find active and passive attackers, attacks based on their intensions where rational attackers seek only personal benefit whereas malicious attackers seek to create obstacles, network attacks where all the network is jeopardized, application attacks where bogus information can be sent, timing attacks which alter messages time slots, and monitoring attacks where intruders monitor the system to later perform an attack. The authors also state several methods to prevent such attacks including:

1. Sybil nodes can be identified since these will be acting in different channels.
2. Bogus information can be prevented by using hashing and asymmetric cryptography.
3. DoS can be prevented by using the IP-CHOCK model where OBUs keep track of IP information and identifying duplicates produced by DoS attacks.
4. Routing attacks can be prevented by using hashing, digital signatures and cryptographic techniques.
5. Eavesdropping is prevented by encrypting sensitive data.
6. Location trailing can be prevented by implementing ID-based security systems.
7. Replay attacks can be attenuated by implementing on each node the use of time stamps and global clock.
8. Session hijacking can be prevented by the use of encryption, and random SID.
9. Timing attacks can be prevented by using a TPM solution.

Table 2
Summary of VANET challenges in the literature.

Challenges	Issues
Absence of peers in VANET	Network congestion, node connection unavailable, overload of information
Attackers	Security Vulnerability, Message Alerts, Sybil Attacks, Privacy Violation
Data Integrity	Authorized users may send malicious data that can lead to accidents
Decentralized	Unauthorized vehicles can join the network, inexistence of centralized authorities
Dynamic Nature	Delayed response time
Error Tolerance	Protocols and algorithms errors can harm VANETs if the former are not designed considering such case
Forwarding Algorithms	Determining best routes is challenging and solutions depend on a combination of broadcast, unicast, V2V, and V2I communication
Key Computation	Strong encryption is required to be used but needs to be balanced with computational capabilities
Key Management	The creation, maintenance, distribution, and update can be jeopardized
Limited Bandwidth	Weak signal, Delayed messages, Network congestion, Interference
Network Size	Limited by the geographical topology, restricted centralized control, short-timed connections, frequent disconnections

Table 3
Compromised security components based on attack type.

Attack class	Compromised security components
Application Attacks	Authentication, confidentiality, integrity, and reliability
Monitoring Attacks	Anonymity and authentication
Network Attacks	Authentication, availability, and integrity
Social Attacks	All
Timing Attacks	Delay handling

Table 4
A snapshot of common attacks and countermeasures.

Common attacks	Security protocols
Bogus and/or Modified Messages	A-SAODV, ECDSA, SAODV
DoS	Ariadne, SEAD, TESLA, TESLA++
Eavesdropping	ARAN
Node Impersonation	ARAN, A-SAODV, ECDSA Holistic-Protocol, SAODV, SEAD
Replay	ARAN, Ariadne
Routing	SEAD, Ariadne, SAODV, A-SAODV
Session hijacking	One Time Cookie
Sybil	RobSAD

The authors' highlighted security solutions to prevent many of the presented attacks include ARAN, SEAD, Ariadne, SAODV, A-SAODV, One Time Cookie, ECDSA, RobSAD, and holistic Protocol.

5.3. Attacks and security solutions

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 depend 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. [89] break down the VANET attack types into network attacks, application attacks, timing attacks, social attacks, and monitoring attacks. Each of these can be accomplished when one or more security components are breached as presented in Table 3.

In order to ensure secured communication within the VANET, a number of node and message authentication schemes have been proposed to counter the diversity of attacks that can be executed by an intruder (a non-legitimate node). Such schemes are used to detect non-legitimate nodes as well as fake messages. Table 4 presents the authentication schemes that can be used to counter specific attacks perpetrated by non-legitimate nodes.

While we might want to take for granted that each of the VANET's components have been properly implemented through the different security entities (Certification Authorities, Road Side Units, and On Board Units), attackers will attempt to do their best to breach them. For each attack, the attack vectors through which attacks can be executed as well as the security components that can be compromised must be considered. In Tables 5–8, the different possible VANET attacks discussed by Mishra et al. [89], Vaibhav et al. [90], Hasrouny et al. [91], Manvi and Tangade [93] have been grouped into different attack vectors. Four attack vectors were identified: Hardware and Software, Infrastructure, Sensors, and Wireless Communications. For each possible attack, we present proposed solutions found in literature and the corresponding security component they satisfy.

Table 5 presents a summary of the hardware and software based attacks that can be executed by hijacking one or more VANET components. Additionally, the tables present proposed solutions in the literature as well as the security components satisfied by each proposal.

Table 6 presents a summary of the infrastructure-based attacks that can be executed by hijacking one or more VANET components. Additionally, the table presents proposed solutions in the literature as well as the security components satisfied by each proposal.

Table 7 presents a summary of the sensor-based attacks that can be executed by hijacking one or more VANET components. Additionally, the table presents proposed solutions in the literature as well as the security components satisfied by each proposal.

Table 8 presents a summary of the wireless communications-based attacks that can be executed by hijacking one or more VANET components. Additionally, the table presents proposed solutions in the literature as well as the security components satisfied by each proposal.

In addition to the presented solutions categorized by attack vector, other authors have surveyed in previous years specific areas on the vulnerabilities of challenges, threats, attacks, and attack solutions in VANETs. Such authors include Fan et al. [153] in 2005, Heijden [154] in 2010, Samara et al. [155] in 2010, Karagiannis et al. [156] in 2011, Song et al. [157] in 2011, Al-kahtani [158] in 2012, Shringar et al. [159] in 2013, Engoulou et al. [160] in 2014, Raiya and Gandhi [161] in 2014, Hoa and Cavalli [162] in 2014, Patel

Please cite this article in press as: G. De La Torre, et al., Driverless vehicle security: Challenges and future research opportunities, Future Generation Computer Systems (2018), https://doi.org/10.1016/j.future.2017.12.041.

Table 5
Hardware and software based attacks, solutions and security components.

Attack type	Solution	Satisfied security components				
		Anonymity	Authentication	Privacy	Integrity	Non-Repudiation
Bogus and/or Modified Messages	Dahiya and Sharma 2001 [94]		✓	✓		
	Calandriello et al. 2007 [95]	✓	✓	✓		✓
	Guo et al. 2007 [96]	✓	✓	✓	✓	✓
	Zhang et al. 2008 [97]	✓	✓	✓	✓	✓
	Zhang et al. 2008 [98]	✓	✓	✓	✓	✓
	Vighnesh et al. 2011 [99]		✓	✓		
	Hao et al. 2011 [100]	✓	✓	✓		
	Shim 2012 [101]	✓	✓	✓	✓	✓
	Hao et al. 2012 [102]		✓	✓		
	Bhavesh et al. 2013 [103]	✓			✓	✓
	Horng et al. 2013 [104]	✓	✓	✓	✓	
	Lin and Li 2013 [105]		✓		✓	
	Shen et al. 2013 [106]		✓	✓		
	Chuang and Lee. 2014 [107]	✓	✓	✓		
	Zhu et al. 2014 [108]	✓	✓	✓	✓	✓
	Caballero-Gil 2016 [109]		✓	✓	✓	
GPS Spoofing	Studer et al. 2009 [110]		✓			✓
	He and Zhu 2012 [111]		✓			
	Engoulou 2013 [112]			✓		
Message Saturation, Spoofing, and Forgery	Blum and Eskandarian 2004 [113]		✓		✓	✓
	Raya et al. 2006 [114]		✓			✓
	ETSI 2010 [115]		✓	✓	✓	✓
	Veque and Johnen 2012 [116]		✓			
	Engoulou 2013 [112]			✓		
	Rajadurai and Jayalakshmi 2013 [117]		✓			
Node Impersonation	Raya and Hubaux 2005 [118]	✓	✓	✓		✓
	Singelee and Preneel 2005 [119]		✓		✓	✓
	Raya et al. 2006 [88]	✓	✓	✓	✓	✓
	Calandriello et al. 2007 [95]	✓	✓	✓		✓
	Guo et al. 2007 [96]	✓	✓	✓	✓	✓
	Lin et al. 2007 [120]		✓	✓	✓	✓
	Zhang et al. 2008 [97]	✓	✓	✓	✓	✓
	Zhang et al. 2008 [98]	✓	✓	✓	✓	✓
	Lin et al. 2008 [121]	✓	✓	✓	✓	
	Manvi et al. 2009 [122]		✓			✓
	Chim et al. 2009 [123]		✓	✓		
	Studer et al. 2009 [110]		✓			✓
	Sun et al. 2010 [124]	✓	✓	✓	✓	✓
	Wasef and Shen 2010 [125]		✓	✓	✓	✓
	Zhang et al. 2010 [126]	✓	✓	✓		✓
	Chim et al. 2010 [127]	✓	✓	✓	✓	
	Vighnesh et al. 2011 [99]		✓	✓		
	Hao et al. 2011 [100]	✓	✓	✓		
	Huang et al. 2011 [128]	✓	✓	✓	✓	
	Shim 2012 [101]	✓	✓	✓	✓	✓
	Hao et al. 2012 [102]		✓	✓		
	Rhim 2012 [129]		✓			
	Lu et al. 2012 [130]		✓	✓		✓
	Bhavesh et al. 2013 [103]	✓			✓	✓
	Horng et al. 2013 [104]	✓	✓	✓	✓	
	Lin and Li 2013 [105]		✓		✓	
	Shen et al. 2013 [106]		✓	✓		
	Wasef and Shen 2013 [131]		✓			✓
	Ravi and Kulkarni 2013 [132]		✓	✓	✓	
	Chuang and Lee. 2014 [107]	✓	✓	✓		
	Zhu et al. 2014 [108]	✓	✓	✓	✓	✓
	Taeho et al. 2014 [133]	✓	✓	✓	✓	
	Jahanian et al. 2015 [134]		✓			
	Li et al. 2015 [135]	✓	✓	✓		✓

(*continued on next page*)

and Jhaveri [163] in 2015, and Kushwaha et al. [164] in 2015. On the other hand, multiple authors have explored the possibility of performing some of the listed attacks in VANETs in either physical or through simulated environments.

Examples include Jafarnejad et al. [165] where the authors showcase a vulnerability analysis on the Renault Twizy electric car that resulted from their findings from a hacking experiment. For the experiment, an Open Vehicle Monitoring System (OVMS) is connected to the On-board Diagnostics (OBD) port providing access to the Controller Area Network (CAN) Bus. The CAN bus is used in the automobile industry to exchange short messages between Electronic Control Units (ECUs) at a speed of 1 Mbps. ECUs like the Engine Control Module (ECM) are used to control other subsystems within an automobile such as the torque, fuel injection system, air intake, etc. By gaining control of such systems, one can start jeopardizing the vehicles security. Some of the advantages exploited using the OVMS were the connectivity provided through GPRS/GSM and serial as well as its GPS. By using the OVMS and CANopen, the team executed a brute force attack into the vehicle's main ECU (Sevcon Gen4), which had four

Please cite this article in press as: G. De La Torre, et al., Driverless vehicle security: Challenges and future research opportunities, Future Generation Computer Systems (2018), https://doi.org/10.1016/j.future.2017.12.041.

Table 5 (*continued*)

Attack type	Solution	Satisfied security components				
		Anonymity	Authentication	Privacy	Integrity	Non-Repudiation
Masquerading	ETSI 2010 [115]		▯	▯	▯	▯
Replay	Lin et al. 2007 [120]		▯	▯	▯	▯
	Zhang et al. 2008 [98]	▯	▯	▯	▯	▯
	ETSI 2010 [115]		▯	▯	▯	▯
	Sun et al. 2010 [124]	▯	▯	▯	▯	▯
	Vighnesh et al. 2011 [99]		▯	▯		
	Rhim 2012 [129]		▯			
	Wasef and Shen 2013 [131]		▯			▯
	Chuang and Lee. 2014 [107]	▯	▯	▯		
	Zhu et al. 2014 [108]	▯	▯	▯	▯	▯
	Taeho et al. 2014 [133]	▯	▯	▯	▯	
Timing	Raya and Hubaux 2005 [118]	▯	▯	▯		▯
	Guette and Bryce 2008 [136]		▯	▯	▯	
	Chuang and Lee. 2014 [107]	▯	▯	▯		

Table 6
Infrastructure-based attacks, solutions and security components.

Attack type	Solution	Satisfied security components				
		Anonymity	Authentication	Privacy	Integrity	Non-Repudiation
Repudiation	Dahiya and Sharma 2001 [94]		▯	▯		
	Singelee and Preneel 2005 [119]		▯		▯	▯
Session Hijacking	Mishra et al. 2015 [137]		▯			
Key-Certificate Replication	Dahiya and Sharma 2001 [94]		▯	▯		
	Raya and Hubaux 2005 [118]	▯	▯	▯		▯
	Raya et al. 2006 [88]	▯	▯	▯	▯	▯
	Rao et al. 2007 [138]					
	Aslam and Zou 2009 [139]		▯	▯		▯

Table 7
Sensor-based attacks, solutions and security components.

Attack type	Solution	Satisfied security components				
		Anonymity	Authentication	Privacy	Integrity	Non-Repudiation
Illusion	ETSI 2010 [115]		▯	▯	▯	▯
	He and Zhu 2012 [111]		▯			
	Engoulou 2013 [112]			▯		
Jamming	Engoulou 2013 [112]			▯		
	Malla and Sahu 2013 [140]					

accessibility levels. Once the maximum accessibility level code was obtained, the team accessed one master Object Dictionary (OD) and proceeded to change some of the parameters within the controller. In addition, the team developed a web interface and an Android App, which permitted them to communicate with the automobile remotely. By examining the responses to the parameters changed in the controller, the team identified the key parameter allowing them to change the throttle pedal position, the gear state, and a form to stop the vehicle (at 30 km/h) by applying a negative torque. The experiment demonstrated the feasibility to hack an all-electric vehicle prominently used in Europe with a relatively easy implementable procedure. Some of the attack scenarios expressed in this paper include changing the speed, force the car to go back or forward, changing the motor's direction. Possible solutions for the presented problem include the implementation of cryptography for authentication through Hardware Security Modules (HSM), challenge-response authentication protocols to deter brute force attacks, IDS on the vehicle's network, and provision of warning flags when an unexpected access to the ECU is detected.

Garip et al. [166] exploit vulnerabilities in VANETs focused on the nature and productions of botnet attacks. Botnets are defined as a collection of vehicles controlled remotely by an infiltrator. Through a simulation using SUMO and OMNeT, the team showcases a botnet communication protocol passing through the VANET network while avoiding detection. Before starting an attack, a botmaster compromises a vehicle and sends/receives password requests and responses through Internet connection for initialization, synchronization and confidentiality purposes. Afterwards, the botmaster will maintain occasional communication with each of the compromised vehicles to maintain an updated list of vehicles under the botnet control to which it can communicate. The attack is transmitted through the VANET's control channel, which is used to transmit vehicle-to-vehicle basic safety messages (BSM) using IEEE's 802.11p protocol. Botnet messages are no different than normal messages in the exercise made and are difficult to identify due to the high network traffic; furthermore, messages are not sent into every BSM and the injection frequency is changes. During each injection, only half a byte is changed from only 4 BSM data items. In this case, the selected data items were the latitude, longitude, position accuracy, transmission and speed in order to avoid rising any flags by changing other more sensitive data items. In addition, precautions were taken to adjust maximum changes to expected natural variations. As an example, speed can only be changed 0.67 mph, position field 0.08 degrees and GPS 24 cm. Furthermore, the botmaster updates passwords given to each infected vehicle every 13 s, thus protecting the botnet from eavesdroppers and brute force attackers to prevent the botnet from being affected. Considered countermeasures to prevent using BSM for transmitting attack information include changing the BSM standard in a manner that they could reject changes that surpass a natural variation threshold. Once a vehicle is under suspicion of being under the control of a botmaster, this could be disconnected

Please cite this article in press as: G. De La Torre, et al., Driverless vehicle security: Challenges and future research opportunities, Future Generation Computer Systems (2018), https://doi.org/10.1016/j.future.2017.12.041.

Table 8
Wireless communications-based attacks, solutions and security components.

Attack type	Solution	Satisfied security components				
		Anonymity	Authentication	Privacy	Integrity	Non-Repudiation
Brute Force	Zeadally et al. 2012 [141]		▯			
Denial of Service	Dahiya and Sharma 2001 [94]		▯	▯		
	Raya and Hubaux 2005 [118]	▯	▯	▯		▯
	Guo et al. 2007 [96]	▯	▯	▯	▯	▯
	Studer et al. 2009 [110]		▯			▯
	He and Zhu 2012 [111]		▯			
	Engoulou 2013 [112]			▯		
	Wasef and Shen 2013 [131]		▯			▯
	Verma et al. 2013 [142]	▯	▯	▯		
	Chuang and Lee. 2014 [107]	▯	▯	▯		
	Zhu et al. 2014 [108]	▯	▯	▯	▯	▯
	Jahanian et al. 2015 [134]		▯			
	Hasrouny et al. 2017 [143]	▯	▯	▯	▯	▯
Eavesdropping	Raya et al. 2006 [114]		▯			▯
	Calandriello et al. 2007 [95]	▯	▯	▯		▯
	Plößl and Federrath 2008 [144]	▯	▯	▯	▯	▯
	Abuelela et al. 2009 [145]		▯	▯		
	Whyte et al. 2013 [146]		▯	▯		
Malware	Singelee and Preneel 2005 [119]		▯		▯	▯
Man in the Middle	Jung et al. 2009 [147]	▯	▯	▯		
	Chuang and Lee. 2014 [107]	▯	▯	▯		
Spam	Singelee and Preneel 2005 [119]		▯		▯	▯
ID-Disclosure	Raya and Hubaux 2005 [118]	▯	▯	▯		▯
	Calandriello et al. 2007 [95]	▯	▯	▯		▯
	Guo et al. 2007 [96]	▯	▯	▯	▯	▯
	Lin et al. 2007 [120]		▯	▯	▯	▯
	Zhang et al. 2008 [97]	▯	▯	▯	▯	▯
	Zhang et al. 2008 [98]	▯	▯	▯	▯	▯
	Chim et al. 2009 [123]		▯	▯		
	Wasef and Chen 2010 [125]		▯	▯	▯	▯
	Zhang et al. 2010 [126]	▯	▯	▯		▯
	Vighnesh et al. 2011 [99]		▯	▯		
	Hao et al. 2011 [100]	▯	▯	▯		
	Huang et al. 2011 [128]	▯	▯	▯	▯	
	Shim 2012 [101]	▯	▯	▯	▯	▯
	Hao et al. 2012 [102]		▯	▯		
	Bhavesh et al. 2013 [103]	▯			▯	▯
	Horng et al. 2013 [104]	▯	▯	▯	▯	
	Shen et al. 2013 [106]		▯	▯		
	Chuang and Lee. 2014 [107]	▯	▯	▯		
	Zhu et al. 2014 [108]	▯	▯	▯	▯	▯
Location Trailing	Raya and Hubaux 2005 [118]	▯	▯	▯		▯
	Calandriello et al. 2007 [95]	▯	▯	▯		▯
	Guo et al. 2007 [96]	▯	▯	▯	▯	▯
	Lin et al. 2007 [120]		▯	▯	▯	▯
	Aslam and Zou 2009 [139]		▯	▯		▯
	ETSI 2010 [115]		▯	▯	▯	▯
	Sun et al. 2010 [124]	▯	▯	▯	▯	▯
	Wasef and Chen 2010 [125]		▯	▯	▯	▯
	Zhang et al. 2010 [126]	▯	▯	▯		▯
	Salem et al. 2010 [148]		▯	▯		▯
	Lu et al. 2012 [130]		▯	▯		▯
	ETSI 2012 [149]	▯	▯	▯		
	Whyte et al. 2013 [146]		▯	▯		
	Chuang and Lee. 2014 [107]	▯	▯	▯		
	Zhu et al. 2014 [108]	▯	▯	▯	▯	▯
	Li et al. 2015 [135]	▯	▯	▯		▯
Sybil	Newsome et al. 2004 [150]					
	Singelee and Preneel 2005 [119]		▯		▯	▯
	Raya et al. 2006 [88]	▯	▯	▯	▯	▯
	Xiao et al. 2006 [151]					
	Vighnesh et al. 2011 [99]		▯	▯		
	Zhou et al. 2011 [152]	▯		▯		
	Shim 2012 [101]	▯	▯	▯	▯	▯
	Lu et al. 2012 [130]		▯	▯		▯
	Bhavesh et al. 2013 [103]	▯			▯	▯
	Li et al. 2015 [135]	▯	▯	▯		▯

from the network. On the other hand, Internet traffic could be also monitored in order to detect a botmaster and block him from further communication to the VANET.

Raya et al. [88] presents an analysis of vulnerabilities on vehicle communications (VC) and the proper design of vehicular communication protocols and systems to prevent abuse and make these

protocols resilient to ongoing attacks. The listed types of vulnerabilities include jamming where an attacker blocks part of the spectrum to prevent communications reaching to vehicles, forgery where an attacker transmits false warnings to nearby vehicles, in-transit traffic tampering where an attacker can drop, corrupt or modify messages, impersonation where an attacker mask itself as another user, privacy violation where user personal information is obtained, and on-board tampering where an attacker can modify data transferred to the OBU. Challenges to effectively deliver security to the network and its users include the network volatility, the vehicle's liability versus users' privacy, time-sensitive applications, the network scale, and the heterogeneity of on-board devices and applications. Considering the previously stated vulnerabilities and challenges, the authors propose an architecture where event data recorders, tamper-proof devices, public key infrastructures, authentication systems, and certificate revocation systems work in conjunction to address them. At the time, some of the open problems included secure positioning, data verification, and DoS resiliency.

5.4. Mitigation strategies

5.4.1. Authentication proposals

As we are able to observe from Tables 4–8, different authors have presented different proposals categorized by attack vector to safeguard different security components from a variety of attacks. These include Raya et al. [88], where the authors propose each user in the VANET to sign selected transmitted messages using a private key provided by certificate authorities, along with the private key's certificate for the purpose of hindering impersonation and in-transit traffic tampering attempts. In addition, the authors integrate certificate revocation using Revocation Protocol of Tamper-Proof Device (RTPD), Revocation Protocol using Compressed Certificate Revocation Lists (RCCRL), and Distributed Revocation Protocol (DRP). In RTPD, tamper-prof-devices storing keys receive a revocation message from certificate authorities; once received, the tamper-proof-device deletes all stored keys and sends an acknowledgment message (ACK) to the certificate authority. If no ACK is received, CA proceeds to broadcast the revocation message through low-speed FM radio. RCCRL is used when only a subset of keys are needed to be revoked or when a vehicle's TPD is unreachable. In such cases, the base stations located near the target vehicle broadcast Compressed Certificate Revocation Lists and these lists are also received by neighboring vehicles of the revoked vehicle. Furthermore, DRP is triggered when multiple vehicles detect misbehavior on a particular vehicle in their location. Afterwards, the certificate is revoked and this is communicated to the CA when a connection is available. The proposed protocols are useful to fight back on-board tampering, impersonation, in-transit traffic tapering, forgery and jamming attacks.

Sunnadkal et al. [167] propose to classify VANETs applications into public safety and private applications. Such applications transmit their data between Road Side Units and vehicles, which both are nodes considered as dedicated short-range communications (DSRC) devices. On the other hand, vehicle manufacturers are focusing on equipping vehicles with On-Board Units (OBU) that would carry relevant data of importance from other vehicles and the road. The proposed architecture works under the assumption that vehicles and RSUs are equipped with Tamper Resistant Devices (TRD) collecting information of sensors within the vehicle, and securing credentials. Credentials are provided by Regional Authorities hosted at RSUs that will help vehicles have short-term credentials even when these are not capable to contact CAs to obtain long-term credentials. In addition, OBUs will be generating pseudonyms, with the help of certificates, for each respective vehicle to mask their IDs as well as creating multiple private/public keys. CAs provide all vehicles with a long-term or permanent unique ID and these are associated to a set of key pairs. Temporary IDs are produced with the generation of pseudonyms using key pairs. The process starts at the OBU where the key pairs are held; these are then sent to the CAs where the verification takes place and a pseudonym is produced and assigned to the vehicle afterwards. Once the temporary ID expires the process is repeated with a new set of key pairs. The CA can trace the identity of a particular pseudonym whenever it is required; it can shut it down and notify nearby vehicles if misbehavior is detected. In the proposed architecture, certificate revocation lists (CRLs) are spread through vehicle-to-vehicle communication instead of only transmitting them through RSUs and OBUs. A non-repudiation process where every transmitted message from the each vehicle is signed by their private key and corroborated on the counterpart with the publicly know public key. Future work involves simulating this architecture using NS2 to observe overheads and efficiency.

5.4.2. Privacy focused proposals

Balancing security and privacy while meeting satisfactory requirements is a key aspect for users within the VANET. Several authors present proposals for safeguarding the privacy of VANET users. These include, Raya et al. [88] where the authors propose to preload CA certified anonymous keys into the tamper-proof-devices. Only one key can be used at a time, these are changed based on the vehicle's driving speed, have short lifetime duration and can only be used once. Additionally, since the CA certifies each key, the vehicle's real identity can be tracked back when needed to determine driver's liability in case of accidents.

Chim et al. [168] defined their VSPN scheme to prevent adversaries from impersonating other vehicles, trace the identity of a targeted vehicle, obtain content of the navigation query made by a vehicle and/or link a query issued by a vehicle with its identity. The summarized assumptions of the authors' scheme are the following:

1. TAs can generate cryptographic operations but they are unknowledgeable of automobiles navigation queries.
2. TAs and tamper-proof systems (installed in vehicles) are assumed to be trusted for managing and generating anonymous credentials.
3. RSUs are not trusted and are unknowledgeable of automobiles navigation queries, RSUs and TAs communicate through secure networks.
4. Vehicle initial authentication is achieved by the use of a PKI where all vehicles hold a public/private keys and are provided with a TA certificate.
5. TAs and RSUs authenticate through a conventional identity-based public key infrastructure and although these two collude they are unable to match a vehicles identity with its issued queries.
6. Pseudo identities are assigned to vehicle's to maintain their identity anonymous to other elements in the network except to trusted authorities (TAs) that have the capability to identify the vehicle if needed based on the pseudo identity.
7. Large amount of queries are assumed to be requested to RSUs, RSUs store neighboring road information and the directions to reach a nearby RSUs.
8. Tamper-proof systems are assumed to be responsible for all cryptographic-related functions and host their own clock used for generating time-stamps.
9. The final assumption consists that RSUs, TAs, and tamper-proof devices have synchronized clocks.

The VSPN scheme is summarized into the following steps:

1. First the TA sets parameters and generate anonymous credentials.

2. The tamper-proof within a vehicle requests the RSU the master secret and a navigation credential afterwards.
3. The RSU replies with a anonymous credential to the tamper-proof device once the vehicles ID is verified.
4. After the vehicle has traveled some distance or a delay has passed it sends a navigation request to the RSU, this request is passed to neighboring RSUs until it reaches the RSU closest to the vehicles destination.
5. The last mentioned RSU defines a navigation and replies it back to the source RSU where during the transmission signed hop information is attached.
6. The source RSU sends this information to the vehicle's taper proof device and validates messages from all RSUs.
7. A navigation session number is generated which is used by the vehicle to obtain navigation information from RSUs along its given path.
8. At the end, the pseudo-identity assigned to a vehicle by an RSU is utilized by the TA to reveal the vehicles true identity for billing purposes.

Simulation showed a minimum processing delay for cryptographic procedures (1.4%–3.3% of the time the vehicle is in querying range of an RSU), a worst case urgent notification time (ranging between 0.1% and 0.3% of the time the vehicle is in querying range of an RSU), and a significant reduction in traveling time (up to a gain ranging from 39% to 55%) compared to the offline map data searching approach, all these results are dependent on the geographical site. Further research seeks for the implementation of the proposed VSPN scheme on a testbed.

5.4.3. Machine learning based proposals

Another approach to provide security within VANETs is achieved through the development of pre-trained models that can be fitted into one of the many interfaces within the network. These pre-trained models take in network traffic to detect anomalies, making abnormal traffic distinguishable from normal traffic and triggering security actions if needed. Examples of this approach include Alheeti et al. [169], where the authors propose an intrusion detection system that combines misuse and anomaly detection systems. As the authors pointed out, some of the VANETs characteristics lead to vulnerabilities within the system; these include, the open wireless medium, the dynamic network topology, and the lack of conventional security infrastructure. By using an NS2 simulator aided with SUMO, MOVE and City Mob software, the team simulated a Manhattan Model (Urban Mobility Model) composed of 30 vehicles and 6 RSUs. With this environment, researchers seek to analyze the impact Denial of Service (DoS) can produce in VANETs where vehicles are sending/receiving Cooperative Awareness Messages (CAMS) to/from other vehicles and RSUs.

DoS attacks can either jam communications or control internal resources; therefore, being capable of attenuating attacks like DOS becomes a critical requirement to insure the wellbeing of the passengers onboard. Initially the team starts by developing the behavior of all vehicles by using NS2 and the dataset by extracting features from the trace file containing network events per vehicle presenting either a normal or a malicious behavior (dropping packets) where the latter is created by modifying routing protocol files. During the simulation, the malicious vehicle is added to the AODV routing protocol producing a trace file different than the one generated by non-malicious vehicles. From the trace file, all 25 captured features are preprocessed by using normalization, transformation, and uniform distribution where every feature is used for training and testing the generated IDS. The IDS is built based on a Feed Forward ANN model consisting of 3 layers where 25 neurons are used in the input layer (1 per feature), 5 neurons in the hidden layer, and 3 neurons in the output layer with a fixed learning rate which common goal is to identify malicious vehicles within the VANET. In total, the dataset consisted in 32,000 records further divided into 3 subsets: training (50%), validation (25%) and test (25%) subsets. The described procedure delivered a training accuracy of 98.97% while during the testing phase an error rate of 2.05% was observed and the rate of alarms (true positive–true negative) where 99.82% and 94.86% respectably. Furthermore, the team expects to extend their research by using a fuzzy data set aiming to lower the error rate and false positives.

Alheeti and McDonald-Maier [170] propose an intrusion detection system based on a Back Propagation ANN. The system aims to differentiate between normal and abnormal traffic within a VANET network, specifically in the exchange of Cooperative Awareness Messages (CAMs) which are shared between vehicles (autonomous or semi-autonomous) and between vehicles and Road Side Units (RSUs). The authors used the Kyoto dataset to which they applied the Proportional Overlapping Technique to eliminate low-impact features, helping to improve performance and detection rate. Afterwards, the significant features pass through a fuzzification process, clearing out classification issues in the dataset. For training and testing, a back propagation ANN is employed consisting in one input layer, hidden layers and one output layer determining normal, abnormal or unknown traffic. The number of optimal layers and neurons is calculated by using cross-validation.

6. In-vehicle communication technologies

In addition to VANET, which main focus surrounds wireless communication, many papers address the security technologies enabling in-vehicle communication. Some of the technologies most automakers include in their produced vehicles to enable communication to ECUs, information displays, infotainment data, among others include: Automotive Ethernet, Byteflight, Controller Area Network (CAN), FlexRay, Local Interconnect Network (LIN), Low-Voltage Differential Signaling (LVDS), and Media Oriented Systems Transport (MOST). An example on how these technologies are implemented within a vehicle is shown in Fig. 3.

Each one of these in-vehicle communication networks deliver a different bitrate and therefore some are preferred to transmit certain types of data rather than others. Amongst the options offering the highest data capacities is the Automotive Ethernet, which is an in-car point-to-point network, offering viable cost and weight reductions. A gigabyte solution of Automotive Ethernet, standardized by IEEE 802.3, can be found as the 1000BASE-T1. Other technologies like NFC and Ultra-Wideband Ranging (UWB) can be utilized to start engines, vehicle access and key location services as these are being rapidly adopted in the automotive market. Table 9 presents a summary of bitrate per protocol as well as their most common applications:

Furthermore, these technologies can be categorized based on their objective into the following: control data, safety data, infotainment data, and driver assistance categories. Zeng et al. [172], Studnia et al. [173], and [174] present detailed information about the challenges, threats, attacks, and solutions encountered in these networks. In Sections 6.1–6.5, a brief summary based on these articles is presented focusing in each n-vehicle network technology. Additional literature proposing solutions for each network, and a table presenting security solutions consolidated by security category is presented.

6.1. Automotive Ethernet

Automotive Ethernet is an emerging network that has gathered the attention of automakers due to its bandwidth and the shared costs with IT and Telecom industries. Despite that Gigabit Ethernet is not suitable for the automobile industry due to the higher cost

Please cite this article in press as: G. De La Torre, et al., Driverless vehicle security: Challenges and future research opportunities, Future Generation Computer Systems (2018), https://doi.org/10.1016/j.future.2017.12.041.

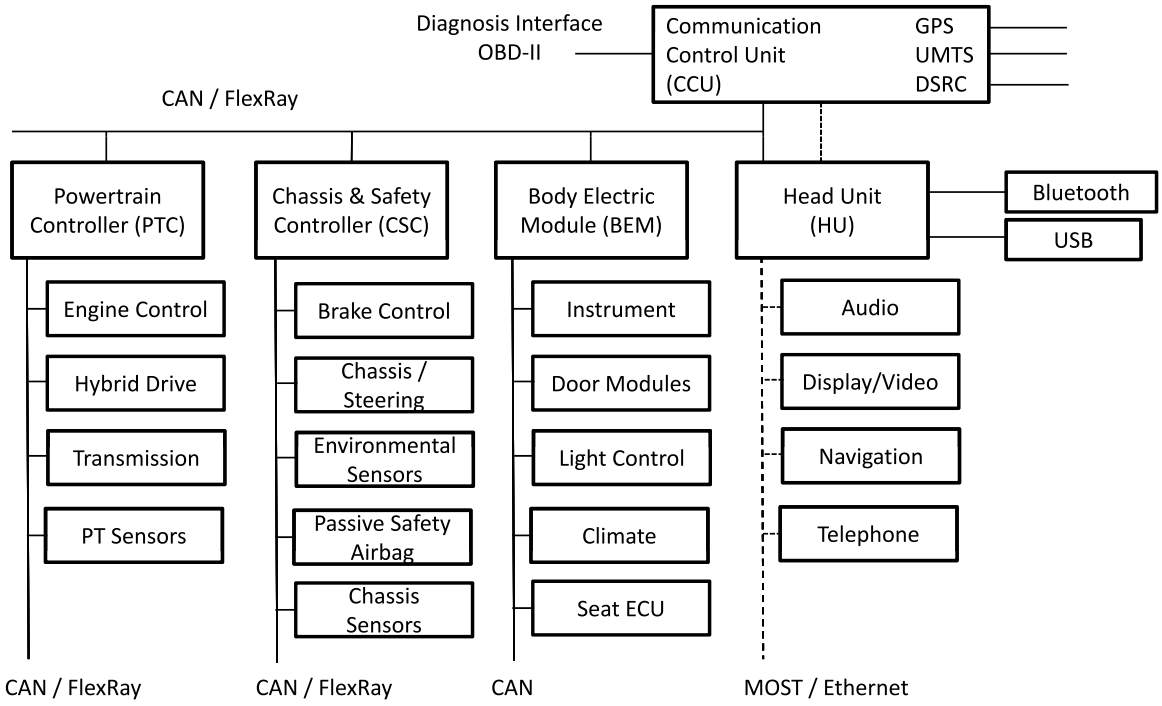


Fig. 3. Automotive on-board network architecture.
Source: adapted from [171].

Table 9
Protocol applications and bitrate summary.

Protocol	Bitrate	Applications
Automotive Ethernet	100 Mbps	Multimedia
FlexRay	20Mbps	Dynamics-Domain and Inter-Domain Communications
CAN	1 Mbps	Powertrain Systems, Upper Body Electronics
LIN	19.2 Kbps	Central Door Lock Activation, Window Lifter Control, Mirror Adjustment, Steering Wheel Button Module, Low Refresh Rate Sensors
LVDS	655 Mbps	In-Vehicle Multimedia
MOST	150 Mbps	In-Vehicle Multimedia, Infotainment

Table 10
Security measures in automotive ethernet.

Category	Solutions
Authentication	MAC, Time Delayed Release of Keys, VLAN
Encryption	AES, ALE, Hybrid Cryptosystem, Zero Latency Encryption
Restricted Physical Access	Point-to-Point Connection Isolation

of processing units, Automobile Ethernet is capable of delivering a bandwidth of 100 Mbps through its supported multi-access full-duplex transmission, which is well suited for ADAS implementation and multimedia delivery. Resiliency in Automotive Ethernet is dependent on transmission media, payload, transmission mode, among others. Table 10 summarizes the range of security measures that could be taken by category.

6.2. FlexRay

FlexRay is an automotive networking standard developed by the FlexRay consortium, which before its dissolution in 2009 was conformed by BMW, Daimler, GM, and Volkswagen. Although FlexRay is capable of providing a greater data rate, flexibility, and deterministic time-triggered TDMA than CAN; FlexRay nodes can be unappealing due to its higher cost [175–177] in contrast with CAN nodes and its complexity to be deployed in automobiles [178]. Another important advantage in FlexRay is its resiliency to errors facilitated by features such as two independent communication channels, signal sampling, coding, decoding, and redundancy check [179]. He et al. present a thorough study on FlexRay implementation in automotive systems [180]. In terms of security, Gang et al. [181] adopted the TESLA protocol and propose divide-and-conquer techniques to solve sub problems in cascade mode, and utilize the two-step approach in two industrial cases. Table 11 summarizes the range of security measures that could be taken by category.

6.3. CAN

CAN is the most widely adopted in-vehicle network technology by automakers to transmit the majority of in-vehicle communications due to its low cost and large requirement within a single unit (up to 500 million chips) [172]. CAN's resiliency is considered as acceptable; its noise-resistance, fault-tolerance, and resistance to external common-mode interference capabilities are provided by its use of unshielded twisted pair lines. Additionally, CAN transceivers nowadays have the capability to detect and report errors in the physical layer. Some of the major drawbacks in CAN are indeterminism, Byzantine General Problem, and the inability to handle Idiot Bubbling Failure. In terms of CAN security Studnia et al. present [173] a study on the bus vulnerabilities found, local

Table 11
Security measures in FlexRay.

Category	Solutions
Authentication	Membership, MAC, Time Delayed Release of Keys
Encryption	AES, ALE, Central Gateway Encryption, Hybrid Cryptosystem, Zero Latency Encryption
Restricted Physical Access	No Exposure

Table 12
Security measures in CAN.

Category	Solutions	Literature
Authentication	Membership, MAC	[187]
Intrusion Detection and Prevention	Anomaly Detection: Signature-Based and Anomaly Based	[188–191]
Encryption	AES, ALE, Central Gateway Encryption, Hybrid Cryptosystem	[182–186]
Restricted Physical Access	Central Gateway Isolation	
Software Security	HSW Module	

attacks, and remote attacks that can be performed in CAN. To prevent such attacks, solutions enabling ECU authentication, integrity check, and transmitted frame encryption are presented by Groza et al. [182], Herrewege et al. [183], and Hartkopp et al. [184]. Furthermore, in order to implement such encryption algorithms over CAN, EVITA developed a security module named Hardware Security Module (HSM) presented by Wolf and Gendrullis in [185], and by Schweppe [186]. Lin and Sangiovanni-Vicentelli [187] present a run-time authentication based mechanism taking into account that an ignition key and security keys have been properly distributed to the ECUs. An anomaly detection approach monitoring delay between frames is presented by Broster and Burns [188]. Binary tainting is used by Schweppe [189] to mark data used by ECUs, enabling to track malicious system intrusions. Other anomaly prevention and detection methods are proposed by Muter et al. [190] who employ a signature-based approach on a sequence of frames and by Muter and Asaj [191] who defines an anomaly-based approach by building a model based on the CANs entropy. In addition to the previously stated models, software integrity occupies a critical place which can be achieved by using mechanisms similar to Arbaugh et al.'s secure boot [192] using modules such as EVITA's HSM. Finally, Pan et al. [193] present a variety of feasible scenarios where a vehicle is no longer safe after the CAN bus is compromised. The authors also present an attack on a modern vehicle with the use of a smart phone, a scenario that should be taken into account due to the increasing computational capabilities of mobile devices and their popularity around the globe. Table 12 summarizes the range of security measures that could be taken by category.

6.4. LIN

LIN is commonly used to transmit communications with low speed where timing performance is not critical. This type of network has become very popular within automakers due to its implementation cost, its use of UART ports making a variety of microcontrollers capable of being used as LIN controllers, and the easy development of its software stack. In addition, LIN's network is constructed based on a linear bus topology operating in a master–slave manner with up to 15 slave nodes recommended for its proper operation. Furthermore, LIN is attractive due to its resiliency of transmission errors by using checksum, parity bit, read back mismatch monitoring, and response error bit. Table 13 summarizes the range of security measures that could be taken by category.

6.5. MOST

MOST networks evolved from the Domestic Digital Bus (D2B) and it has been increasing its adoption in consumer electronic devices and a number of vehicle models [194]. Despite the high cost to equip MOST into a vehicle, mainly increased by the shielding and separation of optical connectors, it is an attractive solution due to its unidirectional logic ring transmission patterns, separated transmitter and receiver, high bandwidth, and involvement of all seven layers in the OSI model. Additionally, MOST is also immune to electromagnetic interference since data is transmitted through optical cables and has a very low data rate, making it the ideal solution for ADAS [195]. Despite of this capability, a single faulty MOST node can lead to a complete network shutdown. Table 14 summarizes the range of security measures that could be taken by category.

Table 13
Security measures in LIN.

Category	Solutions
Authentication	Membership, MAC
Encryption	ALE, Central Gateway Encryption, Hybrid Cryptosystem
Restricted Physical Access	Central gateway Isolation, Restriction to Slave Nodes

Table 14
Security measures in MOST.

Category	Solutions
Authentication	Membership, MAC
Encryption	AES, ALE, Central Gateway Encryption, Hybrid Cryptosystem
Restricted Physical Access	No Exposure

In addition to the presented in-vehicle networks, others such as Byteflight (FlexRay Predecessor), CAN with Flexible Data-Rate (CANFD), Low-Voltage Differential Signaling (LVDS), Vehicle Area Network (VAN), and Time-Triggered CAN (TTCAN) have not been widely adopted by the auto industry as the ones previously presented due to their lack of bandwidth in the case of VAN, affinity to more appealing solutions like FlexRay in the case of Byteflight and TTCAN, the inability to provide both high bandwidth and determinism at the same time in the case of CANFD, or how expensive these can be in auto deployments such as LVDS in contrast with a more appealing inexpensive solution Automotive Ethernet.

7. Concluding remarks

The number of driverless vehicles globally is likely to increase in the foreseeable future and this is likely to create not only a larger potential target for malicious users, but also a potentially larger

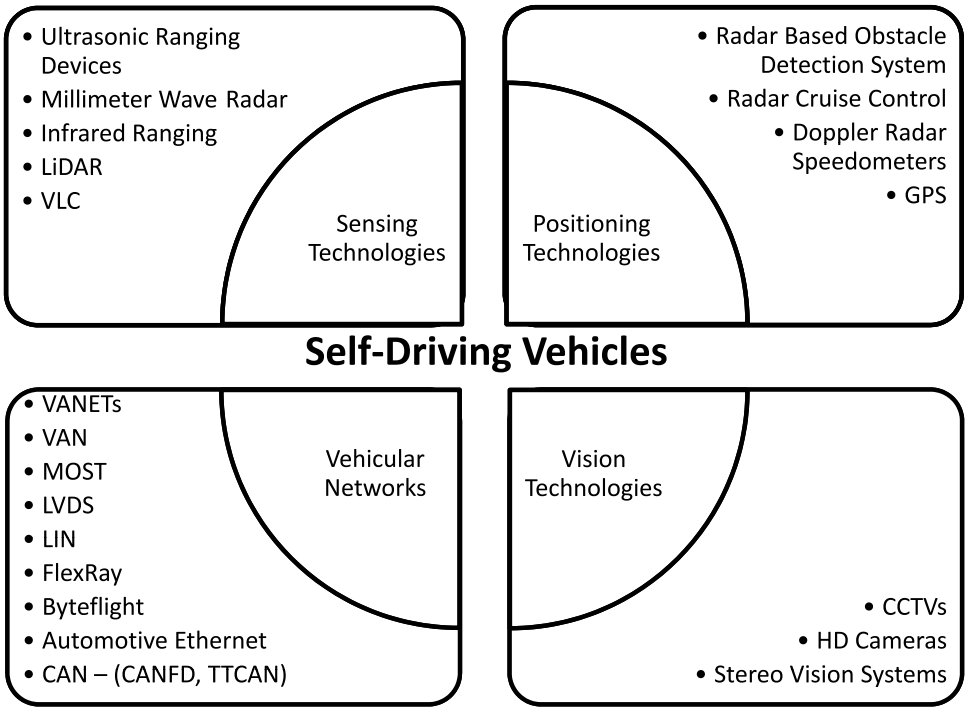


Fig. 4. Technologies equipped in self-driving vehicles.

number of adverse incidents relating to exploitation of vulnerabilities contained in the vehicles.

In this paper, we reviewed and discussed the range of attacks and security concerns that can affect the different technologies that underpinned self-driving vehicles—see Fig. 4. For example, we revealed that LiDAR systems could either be the target of the attack or become the source of the attack by modifying embedded lasers. We also explored the capabilities of VLC and concluded that attacks on this technology must be executed through a LOS based on the literature available.

We then reviewed how GPS spoofing could be performed, and described mitigation strategies, and functionality restoration proposals. In addition, radar based systems, capable of complimenting GPS functionality, were introduced. We also examined the stereo vision systems as well as security methods utilized in other vision technologies that could be implemented on these. Security methods included active video forgery detection using watermarking as well as passive video forgery detection. Our discussion of vehicle networks focused on VANETs and In-Vehicle Networks. In VANETS, we 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. In addition, an in-depth explanation of the different mitigation strategies was presented. For in-vehicle networks, the different networking technologies that have been equipped in different vehicle models were presented. We reviewed existing capability differences and the range of applications each can cover. Based on this, we presented different security solutions that can be implemented for each technology and found literature supporting such statements. We then summarized the different technologies that can be equipped in self-driving vehicles to enable them to reach a desired autonomy level.

Generally, efforts have been devoted to address security and privacy concerns present in driverless vehicles, although future efforts should be more holistic and coordinated. However, cyber protections are seldom absolute. As explained in [196] p. 108, "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. IoT and vehicle forensics are relatively new [197–199], 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 [200–203]). 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 [196,204,205] to the development of future driverless vehicles. This also echoes the observations of Huang, Lu and Choo [206] and Lin et al. [207] who recently noted the importance of having forensically ready/friendly vehicular fog computing systems and Internet of Drones.

Acknowledgments

The authors thank the editor and the anonymous reviewers for their constructive feedback. The last author is supported by the Cloud Technology Endowed Professorship.

References

[1] CNN, Terrorist Attacks by Vehicle Fast Facts, 2017. http://www.cnn.com/2017/05/03/world/terrorist-attacks-by-vehicle-fast-facts/index.html. (Accessed 5 October 2017).
[2] N. Highway Traffic Safety Administration, N. Center for Statistics, Traffic Safety Facts 2015, 2015. http://dx.doi.org/10.1016/j.annemergmed.2013.12.004.
[3] S. Brandon, M. Sivak, A Survey of Public Opinion About Autonomous and Self-Driving Vehicles in the U.S. the U.K. and Australia, 2014, p. 40. http://dx.doi.org/10.1109/ICCVE.2014.45.
[4] J. Petit, S.E. Shladover, Potential cyberattacks on automated vehicles, IEEE Trans. Intell. Transp. Syst. (2014) 546–556. http://dx.doi.org/10.1109/TITS.2014.2342271.
[5] K. Sjoberg, P. Andres, T. Buburuzan, A. Brakemeier, Cooperative intelligent transport systems in Europe: Current deployment status and outlook, IEEE Veh. Technol. Mag. 12 (2017) 89–97. http://dx.doi.org/10.1109/MVT.2017.2670018.

[6] F. Zhang, D. Clarke, A. Knoll, Vehicle detection based on lidar and camera fusion, in: 17th Int. IEEE Conf. Intell. Transp. Syst., IEEE, 2014, pp. 1620–1625. http://dx.doi.org/10.1109/ITSC.2014.6957925.
[7] N. Gallardo, N. Gamez, P. Rad, M. Jamshidi, Autonomous decision making for a driver-less car, in: 2017 12th Syst. Syst. Eng. Conf, IEEE, Waikoloa, Hawai, 2017, pp. 1–6. http://dx.doi.org/10.1109/SYSOSE.2017.7994953.
[8] R.E. Latta, H.R.3388 - SELF DRIVE Act, Congr. Bill. 115th Cong, 2017.
[9] Updated: Autonomous driving levels 0 to 5: Understanding the differences - TechRepublic, (n.d.). https://www.techrepublic.com/article/autonomous-driving-levels-0-to-5-understanding-the-differences/. (Accessed 21 June 2017).
[10] G. Loukas, C. Patrikakis, Cyber and physical threats to the Internet of Everything, Cut. IT J. 29 (2016) 5–11.
[11] L. Reger, 14 the road ahead for securely-connected cars, in: Dig. Tech. Pap. - IEEE Int. Solid-State Circuits Conf, IEEE, San Francisco, CA, USA, 2016, p. N/A, http://dx.doi.org/10.1109/ISSCC.2016.7417892.
[12] N.O. and A.A. US Department of Commerce, What is LIDAR, (n.d.). http://oceanservice.noaa.gov/facts/lidar.html (Accessed 20 June 2017).
[13] M. Zhao, A. Mammeri, A. Boukerche, Distance measurement system for smart vehicles, in: 2015 7th Int. Conf. New Technol. Mobil. Secur., IEEE, 2015, pp. 1–5. http://dx.doi.org/10.1109/NTMS.2015.7266486.
[14] C. Boehlau, J. Hipp, Optoelectric sensing device with common deflection device, US7345271 B2, 2003. https://www.google.com/patents/US7345271. (Accessed 20 June 2017).
[15] Velodyne LiDAR HDL-64E S3 High Definition Real-Time 3D LiDAR, 2017. http://velodynelidar.com/docs/datasheet/63-9194_Rev-F_HDL-64E_S3_Data~Sheet_Web.pdf.
[16] R. Felix, J. Economou, K. Knowles, Driverless Vehicles and LIDAR : Evaluation of Possible Security Threats on the Open Road, SAE Tech. Pap. 2015-01-0219, 2015. http://dx.doi.org/10.4271/2015-01-0219.Copyright.
[17] U.S. Census Bureau, Cumulative Percent Distribution of Population by Height and Sex: 2007–2008, 2012. http://www.cdc.gov/nchs/nhanes.htm.
[18] M.D. Harris, A.E. Lincoln, P.J. Amoroso, B. Stuck, D. Sliney, Laser eye injuries in military occupations, Aviat. Space. Environ. Med. 74 (2003) 947–952. http://dx.doi.org/10.3357/AMHP.4740.2017.
[19] C. Tuchinda, S. Srivannaboon, H.W. Lim, Photoprotection by window glass, automobile glass, and sunglasses, J. Am. Acad. Dermatol. 54 (2006) 845–854. http://dx.doi.org/10.1016/j.jaad.2005.11.1082.
[20] M. Hashem Eiza, Q. Ni, Driving with sharks: Rethinking connected vehicles with vehicle cybersecurity, IEEE Veh. Technol. Mag. 12 (2017) 45–51. http://dx.doi.org/10.1109/MVT.2017.2669348.
[21] Self-driving cars can be hacked using a laser pointer - Telegraph, (n.d.). http://www.telegraph.co.uk/technology/news/11850373/Self-driving-cars-can-be-hacked-using-a-laser-pointer.html. (Accessed 21 June 2017).
[22] S. Ucar, S.C. Ergen, O. Ozkasap, Security vulnerabilities of IEEE 80211p and visible light communication based platoon, in: 2016 IEEE Veh. Netw. Conf., IEEE, Columbus, OH, USA, 2016. http://dx.doi.org/10.1109/VNC.2016.7835972.
[23] S. Kitano, S. Haruyama, M. Nakagawa, LED road illumination communications system, in: 2003 IEEE 58th Veh. Technol. Conf. VTC 2003-Fall, vol.5, IEEE, Orlando, FL, USA, 2003, pp. 3346–3350. http://dx.doi.org/10.1109/VETECF.2003.1286302.
[24] N. Kumar, Smart and intelligent energy efficient public illumination system with ubiquitous communication for smart city, in: 2013 IEEE Int. Conf. SMART Struct. Syst., IEEE, Chennai, India, 2013, pp. 152–157. http://dx.doi.org/10.1109/ICSSS.2013.6623018.
[25] N. Kumar, N. Lourenco, D. Terra, L.N. Alves, R.L. Aguiar, Visible light communications in intelligent transportation systems, in: 2012 IEEE Intell. Veh. Symp., IEEE, Alcala de Henares, Spain, 2012, pp. 748–753. http://dx.doi.org/10.1109/IVS.2012.6232282.
[26] A. Cailean, B. Cagneau, L. Chassagne, S. Topsu, Y. Alayli, M. Dimian, A robust system for visible light communication, in: 2013 IEEE 5th Int. Symp. Wirel. Veh. Commun., IEEE, Dresden, Germany, 2013, pp. 1–5. http://dx.doi.org/10.1109/wivec.2013.6698223.
[27] A.-M. Cailean, B. Cagneau, L. Chassagne, S. Topsu, Y. Alayli, M. Dimian, Visible light communications cooperative architecture for the intelligent transportation system, in: 2013 IEEE 20th Symp. Commun. Veh. Technol. Benelux, IEEE, Namur, Belgium, 2013, pp. 1–5. http://dx.doi.org/10.1109/SCVT.2013.6736001.
[28] S. Okada, T. Yendo, T. Yamazato, T. Fujii, M. Tanimoto, Y. Kimura, On-vehicle receiver for distant visible light road-to-vehicle communication, in: 2009 IEEE Intell. Veh. Symp., IEEE, 2009, pp. 1033–1038. http://dx.doi.org/10.1109/IVS.2009.5164423.
[29] T. Saito, S. Haruyama, M. Nakagawa, A new tracking method using image sensor and photo diode for visible light road-to-vehicle communication, in: 2008 10th Int. Conf. Adv. Commun. Technol., IEEE, Gangwon-Do, South Korea, 2008, pp. 673–678. http://dx.doi.org/10.1109/ICACT.2008.4493850.
[30] A. Cailean, B. Cagneau, L. Chassagne, S. Topsu, Y. Alayli, J.-M. Blosseville, Visible light communications: application to cooperation between vehicles and road infrastructures, in: 2012 IEEE Intell. Veh. Symp., IEEE, Alcala de Henares, Spain, 2012, pp. 1055–1059. http://dx.doi.org/10.1109/IVS.2012.6232225.
[31] D.-R. Kim, S.-H. Yang, H.-S. Kim, Y.-H. Son, S.-K. Han, Outdoor visible light communication for inter- vehicle communication using controller area network, in: 2012 Fourth Int. Conf. Commun. Electron, IEEE, Hue, Vietnam, 2012, pp. 31–34. http://dx.doi.org/10.1109/CCE.2012.6315865.
[32] L.-H. Yoo, R. Lee, J.-K. Oh, H.-W. Seo, J.-Y. Kim, H.-C. Kim, S.-Y. Jung, Demonstration of vehicular visible light communication based on LED headlamp, in: 2013 Fifth Int. Conf. Ubiquitous Futur. Networks, IEEE, Da Nang, Vietnam, 2013, pp. 465–467. http://dx.doi.org/10.1109/ICUFN.2013.6614862.
[33] I. Takai, S. Ito, K. Yasutomi, K. Kagawa, M. Andoh, S. Kawahito, LED and CMOS image sensor based optical wireless communication system for automotive applications, IEEE Photon. J. 5 (2013) 6801418. http://dx.doi.org/10.1109/JPHOT.2013.2277881.
[34] A. Jovicic, J. Li, T. Richardson, Visible light communication: opportunities, challenges and the path to market, IEEE Commun. Mag. 51 (2013) 26–32. http://dx.doi.org/10.1109/MCOM.2013.6685754.
[35] P.H. Pathak, X. Feng, P. Hu, P. Mohapatra, Visible light communication, networking, and sensing: A survey, potential and challenges, IEEE Commun. Surv. Tutor. 17 (2015) 2047–2077. http://dx.doi.org/10.1109/COMST.2015.2476474.
[36] S. Bittl, A.A. Gonzalez, M. Myrtus, H. Beckmann, S. Sailer, B. Eissfeller, Emerging attacks on VANET security based on GPS Time Spoofing, in: 2015 IEEE Conf. Commun. Netw. Secur., IEEE, Florence, Italy, 2015, pp. 344–352. http://dx.doi.org/10.1109/CNS.2015.7346845.
[37] B.M. Ledvina, W.J. Bencze, B. Galusha, I. Miller, An in-line anti-spoofing device for legacy civil GPS receivers, in: Proc. 2010 Int. Tech. Meet. Inst. Navig. San Diego, CA, 2010, pp. 698–712. https://www.ion.org/publications/abstract.cfm?articleID=8852.
[38] B.M. Ledvina, P. Montgomery, T. Humphreys, A multi-antenna defense: Receiver-autonomous GPS spoofing detection, Insid. GNSS. 2009. http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:A+Multi-Antenna+Defense:+Receiver-Autonomous+GPS+Spoofing+Detection#0%5Cnhttp://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:A+multi-antenna+defense:+Receiver-autonomous+GPS+spoofing+.
[39] M. Meurer, A. Konovaltsev, M. Cuntz, C. Hättich, Robust joint multi-antenna spoofing detection and attitude estimation using direction assisted multiple hypotheses RAIM, in: Robust Jt. Multi-Antenna Spoofing Detect. Attitude Estim. Using Dir. Assist. Mult. Hypotheses RAIM, Nashville, TN, USA, 2012: pp. 3007–3016. https://www.ion.org/publications/abstract.cfm?articleID=10480 (Accessed 5 July 2017).
[40] J.S. Warner, R.G. Johnston, GPS spoofing countermeasures, Homel. Secur. J. 25 (2003) 19–27. http://library.lanl.gov/cgi-bin/getfile?00852243.pdf.
[41] N.O. Tippenhauer, C. Pöpper, K.B. Rasmussen, S. Capkun, On the requirements for successful GPS spoofing attacks, in: Proc. 18th ACM Conf. Comput. Commun. Secur., ACM, New York, New York, USA, 2011, p. 75. http://dx.doi.org/10.1145/2046707.2046719.
[42] A.J. Kerns, D.P. Shepard, J.A. Bhatti, T.E. Humphreys, Unmanned aircraft capture and control via GPS spoofing, J. F. Robot. 31 (2014) 617–636. http://dx.doi.org/10.1002/rob.21513.
[43] M.L. Psiaki, B.W. O'Hanlon, J.A. Bhatti, D.P. Shepard, T.E. Humphreys, Gps spoofing detection via dual-receiver correlation of military signals, IEEE Trans. Aerosp. Electron. Syst. 49 (2013) 2250–2267. http://dx.doi.org/10.1109/TAES.2013.6621814.
[44] D.J. Jwo, F.C. Chung, K.L. Yu, Gps/ins integration accuracy enhancement using the interacting multiple model nonlinear filters, J. Appl. Res. Technol. 11 (2013) 496–509. http://dx.doi.org/10.1016/S1665-6423(13)71557-8.
[45] S.C. Stubberud, K.A. Kramer, Analysis of fuzzy evidence accrual security approach To GPS systems, in: 2014 10th Int. Conf. Commun. IEEE, Bucharest, Romania, 2014, pp. 1–6. http://dx.doi.org/10.1109/ICComm.2014.6866695.
[46] S.C. Stubberud, K.A. Kramer, Threat assessment for GPS navigation, in: 2014 IEEE Int. Symp. Innov. Intell. Syst. Appl. Proc., IEEE, Alberobello, Italy, 2014, pp. 287–292. http://dx.doi.org/10.1109/INISTA.2014.6873632.
[47] B. Anouar, B. Mohammed, G. Abderrahim, B. Mohammed, Vehicular navigation spoofing detection based on V2I calibration, in: 2016 4th IEEE Int. Colloq. Inf. Sci. Technol., IEEE, Tangier, Morocco, 2016, pp. 847–849. http://dx.doi.org/10.1109/CIST.2016.7805006.
[48] J. Magiera, R. Katulski, Detection and mitigation of gps spoofing based on antenna array processing, J. Appl. Res. Technol. 13 (2015) 45–57. http://dx.doi.org/10.1016/S1665-6423(15)30004-3.
[49] D.P. Shepard, T.E. Humphreys, A.A. Fansler, Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks, Int. J. Crit. Infrastruct. Prot. 5 (2012) 146–153. http://dx.doi.org/10.1016/j.ijcip.2012.09.003.
[50] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, G. Lachapelle, rard, GPS vulnerability to spoofing threats and a review of antispoofing techniques, Int. J. Navig. Obs. 2012 (2012) 1–16. http://dx.doi.org/10.1155/2012/127072.
[51] D.de O. Gonçalves, D.G. Costa, A survey of image security in wireless sensor networks, J. Imaging 1 (2015) 4–30. http://dx.doi.org/10.3390/jimaging1010004.

Please cite this article in press as: G. De La Torre, et al., Driverless vehicle security: Challenges and future research opportunities, Future Generation Computer Systems (2018), https://doi.org/10.1016/j.future.2017.12.041.

[52] G.V.S. Raju, R. Akbani, Elliptic curve cryptosystem and its applications, in: SMC'03 Conf. Proceedings. 2003 IEEE Int. Conf. Syst. Man Cybern. Conf. Theme - Syst. Secur. Assur. (Cat. No.03CH37483), IEEE, Washington, DC, USA, 2003, pp. 1540–1543. http://dx.doi.org/10.1109/ICSMC.2003.1244630.

[53] Y. Sadourny, V. Conan, A proposal for supporting selective encryption in JPSEC, IEEE Trans. Consum. Electron. 49 (2003) 846–849. http://dx.doi.org/10.1109/TCE.2003.1261164.

[54] R. Pfarrhofer, A. Uhl, Selective image encryption using JBIG, in: Commun. Multimed. Secur., Springer-Verlag Berlin Heidelberg, Salzburg, Austria, 2005, pp. 98–107. http://dx.doi.org/10.1007/11552055.

[55] J.-L. Liu, Efficient selective encryption for JPEG 2000 images using private initial table, Pattern Recognit. 39 (2006) 1509–1517. http://dx.doi.org/10.1016/j.patcog.2006.02.013.

[56] M. Podesser, H.-P. Schmidt, A. Uhl, Selective bitplane encryption for secure transmission of image data in mobile environments, in: Proc. 5th IEEE Nord. Signal Process. Symp. TromsoTrondheim, Norway, 2002, pp. 1–20.

[57] S.K. Naveenkumar, H.T. Panduranga, Kiran, partial image encryption for smart camera, in: 2013 Int. Conf. Recent Trends Inf. Technol., IEEE, Chennai, India, 2013, pp. 126–132. http://dx.doi.org/10.1109/ICRTIT.2013.6844192.

[58] W. Wang, M. Hempel, D. Peng, H. Wang, H. Sharif, H.-H. Chen, On energy efficient encryption for video streaming in wireless sensor networks, IEEE Trans. Multimed. 12 (2010) 417–426. http://dx.doi.org/10.1109/TMM.2010.2050653.

[59] T. Xiang, C. Yu, F. Chen, Fast encryption of JPEG 2000 images in wireless multimedia sensor networks, in: Int. Conf. Wirel. Algorithms, Syst. Appl, Springer, Berlin, Heidelberg, Zhangjiajie, China, 2013, pp. 196–205. http://dx.doi.org/10.1007/978-3-642-39701-1_17.

[60] B. Harjito, V. Potdar, J. Singh, Watermarking technique for wireless multimedia sensor networks: a state of the art, in: Proc. CUBE Int. Inf. Technol. Conf. - CUBE '12, ACM Press, New York, New York, USA, 2012, pp. 832–840. http://dx.doi.org/10.1145/2381716.2381873.

[61] B. Harjito, V. Potdar, J. Singh, Watermarking technique for wireless sensor networks: A state of the art, in: 2012 Eighth Int. Conf. Semant. Knowl. Grids, IEEE, Beijing, China, 2012, pp. 253–256. http://dx.doi.org/10.1109/SKG.2012.56.

[62] X. Shi, D. Xiao, A reversible watermarking authentication scheme for wireless sensor networks, Inf. Sci. (Ny). 240 (2013) 173–183. http://dx.doi.org/10.1016/j.ins.2013.03.031.

[63] R. Xiao, X. Sun, Y. Yang, Copyright protection in wireless sensor networks by watermarking, in: 2008 Int. Conf. Intell. Inf. Hiding Multimed. Signal Process, IEEE, Harbin, China, 2008, pp. 7–10. http://dx.doi.org/10.1109/IIH-MSP.2008.139.

[64] B. Harjito, S. Han, V. Potdar, E. Chang, M. Xie, Secure communication in wireless multimedia sensor networks using watermarking, in: 4th IEEE Int. Conf. Digit. Ecosyst. Technol., IEEE, Dubai, United Arab Emirates, 2010, pp. 640–645. http://dx.doi.org/10.1109/DEST.2010.5610580.

[65] P. Yu, S. Yao, J. Xu, Y. Zhang, Y. Chang, Copyright protection for digital image in wireless sensor network, in: 2009 5th Int. Conf. Wirel. Commun. Netw. Mob. Comput, IEEE, Beijing, China, 2009, pp. 1–4. http://dx.doi.org/10.1109/WICOM.2009.5305347.

[66] H. Wang, Communication-resource-aware adaptive watermarking for multimedia authentication in wireless multimedia sensor networks, J. Supercomput. 64 (2013) 883–897. http://dx.doi.org/10.1007/s11227-010-0500-5.

[67] A.W.A. Wahab, M.A. Bagiwa, M.Y.I. Idris, S. Khan, Z. Razak, M.R.K. Ariffin, Passive video forgery detection techniques: A survey, in: 2014 10th Int. Conf. Inf. Assur. Secur., IEEE, Okinawa, Japan, 2014, pp. 29–34. http://dx.doi.org/10.1109/ISIAS.2014.7064616.

[68] A. De, H. Chadha, S. Gupta, Detection of forgery in digital video, 10th World Multi-Conference Syst. Cybern. Informatics. V, 2006, pp. 229–233. http://sparshgupta.name/publications/Detection_of_Forgery_in_Digital_Video.pdf.

[69] Chih-Chung Hsu, Tzu-Yi Hung, Chia-Wen Lin, Chiou-Ting Hsu, Video forgery detection using correlation of noise residue, in: 2008 IEEE 10th Work. Multimed. Signal Process, IEEE, Cairns, Qld, Australia, 2008, pp. 170–174. http://dx.doi.org/10.1109/MMSP.2008.4665069.

[70] M. Kobayashi, T. Okabe, Y. Sato, Detecting video forgeries based on noise characteristics, in: Pacific-Rim Symp. Image Video Technol., Springer, Berlin, Heidelberg, Tokyo, Japan, 2009, pp. 306–317. http://dx.doi.org/10.1007/978-3-540-92957-4_27.

[71] J. Zhang, Y. Su, M. Zhang, Exposing digital video forgery by ghost shadow artifact, in: Proc. First ACM Work. Multimed. Forensics - MiFor '09, ACM Press, New York, New York, USA, 2009, p. 49. http://dx.doi.org/10.1145/1631081.1631093.

[72] S.V. Porter, M. Mirmehdi, B.T. Thomas, Video cut detection using frequency domain correlation, in: Proc. 15th Int. Conf. Pattern Recognition. ICPR-2000, IEEE Comput. Soc., Barcelona, Spain, 2000, pp. 409–412. http://dx.doi.org/10.1109/ICPR.2000.903571.

[73] W. Wang, H. Farid, Exposing digital forgeries in video by detecting duplication, in: Proc. 9th Work. Multimed. Secur. - MM&Sec '07, ACM Press, New York, New York, USA, 2007, p. 35. http://dx.doi.org/10.1145/1288869.1288876.

[74] W. Wang, H. Farid, Exposing digital forgeries in interlaced and deinterlaced video, IEEE Trans. Inf. Forensics Secur. 2 (2007) 438–449. http://dx.doi.org/10.1109/TIFS.2007.902661.

[75] P. Bestagini, S. Milani, M. Tagliasacchi, S. Tubaro, Local tampering detection in video sequences, in: 2013 IEEE 15th Int. Work. Multimed. Signal Process, IEEE, Pula, Italy, 2013, pp. 488–493. http://dx.doi.org/10.1109/MMSP.2013.6659337.

[76] N. Dalal, B. Triggs, Histograms of oriented gradients for human detection, in: 2005 IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit., IEEE, San Diego, CA, USA, 2005, pp. 886–893. http://dx.doi.org/10.1109/CVPR.2005.177.

[77] D.-K. Hyun, S.-J. Ryu, H.-Y. Lee, H.-K. Lee, Detection of upscale-crop and partial manipulation in surveillance video based on sensor pattern noise, Sensors 13 (2013) 12605–12631. http://dx.doi.org/10.3390/s130912605.

[78] A.V. Subramanyam, S. Emmanuel, Video forgery detection using hog features and compression properties, in: 2012 IEEE 14th Int. Work. Multimed. Signal Process, IEEE, Banff, AB, Canada, 2012, pp. 89–94. http://dx.doi.org/10.1109/MMSP.2012.6343421.

[79] D. Scharstein, R. Szeliski, High-accuracy stereo depth maps using structured light, in: 2003 IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognition, 2003 Proceedings, IEEE Comput. Soc., Madison, WI, USA, 2003 n.d.: p. I-195-I-202, http://dx.doi.org/10.1109/CVPR.2003.1211354.

[80] V. Couture, N. Martin, S. Roy, Unstructured light scanning to overcome interreflections, in: 2011 Int. Conf. Comput. Vis., IEEE, Barcelona, Spain, 2011, pp. 1895–1902. http://dx.doi.org/10.1109/ICCV.2011.6126458.

[81] T. Kerstein, M. Laurowski, P. Klein, M. Weyrich, H. Roth, J. Wahrburg, Optical 3D-surface reconstruction of weak textured objects based on an approach of disparity stereo inspection, in: Proc. Int. Conf. Pattern Recognit. Comput. Vis. Amsterdam, Netherlands, 2011, pp. 581–586.

[82] Bosch stereo video camera enhances comfort and safety - Bosch Media Service, 2012. http://www.bosch-presse.de/pressportal/de/en/bosch-stereo-video-camera-enhances-comfort-and-safety-41988.html (Accessed June 21, 2017).

[83] U. Seger, U. Apel, Stereo camera arrangement in a vehicle, EP2474451 A1, 2012. https://www.google.com/patents/EP2474451A1?cl=en (Accessed June 21, 2017).

[84] A. Mammeri, A. Boukerche, M. Zhao, Keypoint-based binocular distance measurement for pedestrian detection system, in: Proc. Fourth ACM Int. Symp. Dev. Anal. Intell. Veh. Networks Appl. - DIVANet '14, ACM Press, New York, New York, USA, 2014, pp. 9–15. http://dx.doi.org/10.1145/2656346.2656365.

[85] C. Hassapis, H.K. Nishihara, Stereo camera intrusion detection system, US 8432448 B2, 2013. https://www.google.com/patents/US8432448.

[86] M.O. Obu, M.-O.B.U. Family, MobiWAVE On-Board-Unit (OBU), (n.d.). http://savari.net/technology/on-board-unit/.

[87] W. Liang, Z. Li, H. Zhang, S. Wang, R. Bie, Vehicular Ad Hoc networks: Architectures, research issues, methodologies, challenges, and trends, Int. J. Distrib. Sens. Netw. (2015) N/A. http://dx.doi.org/10.1155/2015/745303.

[88] M. Raya, P. Papadimitratos, J. Hubaux, Securing vehicular communications, IEEE Wirel. Commun. 13 (2006). http://dx.doi.org/10.1109/WC-M.2006.250352.

[89] R. Mishra, A. Singh, R. Kumar, VANET security: Issues, challenges and solutions, in: 2016 Int. Conf. Electr. Electron. Optim. Tech., IEEE, Chennai, India, 2016, p. N/A, http://dx.doi.org/10.1109/ICEEOT.2016.7754846.

[90] A. Vaibhav, D. Shukla, S. Das, S. Sahana, P. Johri, Security challenges, authentication , application and trust models for vehicular ad hoc network- A survey, I, J. Wirel. Microw. Technol. (2017) 36–48. http://dx.doi.org/10.5815/ijwmt.2017.03.04.

[91] H. Hasrouny, A.E. Samhat, C. Bassil, A. Laouiti, VANet security challenges and solutions: A survey, Veh. Commun. 7 (2017) 7–20. http://dx.doi.org/10.1016/j.vehcom.2017.01.002.

[92] H. Hartenstein, K.P. Laberteaux, A tutorial survey on vehicular ad hoc networks, IEEE Commun. Mag. 46 (2008). http://dx.doi.org/10.1109/MCOM.2008.4539481.

[93] S.S. Manvi, S. Tangade, A survey on authentication schemes in VANETs for secured communication, Veh. Commun. 9 (2017) 19–30. http://dx.doi.org/10.1016/j.vehcom.2017.02.001.

[94] A. Dahiya, V. Sharma, A survey on securing user authentication in vehicular ad hoc networks, Int. J. Inf. Secur. 1 (2001).

[95] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, A. Lioy, Efficient and robust pseudonymous authentication in VANET, in: Proc. Fourth ACM Int. Work. Veh. Ad Hoc Networks - VANET '07, ACM Press, New York, New York, USA, 2007, p. 19. http://dx.doi.org/10.1145/1287748.1287752.

[96] J. Guo, J.P. Baugh, S. Wang, A group signature based secure and privacy-preserving vehicular communication framework, in: 2007 Mob. Netw. Veh. Environ., IEEE, 2007, pp. 103–108. http://dx.doi.org/10.1109/MOVE.2007.4300813.

[97] C. Zhang, R. Lu, X. Lin, P.-H. Ho, X. Shen, An efficient identity-based batch verification scheme for vehicular sensor networks, in: IEEE INFOCOM 2008 -

27th Conf. Comput. Commun., IEEE, Phoenix, AZ, USA, 2008, pp. 246–250. http://dx.doi.org/10.1109/INFOCOM.2008.58.

[98] C. Zhang, X. Lin, R. Lu, P.-H. Ho, X. Shen, An efficient message authentication scheme for vehicular communications, IEEE Trans. Veh. Technol. 57 (2008) 3357–3368. http://dx.doi.org/10.1109/TVT.2008.928581.

[99] N.V. Vighnesh, N. Kavita, S.R. Urs, S. Sampalli, A novel sender authentication scheme based on hash chain for vehicular ad-hoc networks, in: 2011 IEEE Symp. Wirel. Technol. Appl., IEEE, Langkawi, Malaysia, 2011, pp. 96–101. http://dx.doi.org/10.1109/ISWTA.2011.6089388.

[100] Y. Hao, Y. Cheng, C. Zhou, W. Song, A distributed key management framework with cooperative message authentication in VANETs, IEEE J. Sel. Areas Commun. 29 (2011) 616–629. http://dx.doi.org/10.1109/JSAC.2011.110311.

[101] K.-A. Shim, CPAS: An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks, IEEE Trans. Veh. Technol. 61 (2012) 1874–1883. http://dx.doi.org/10.1109/TVT.2012.2186992.

[102] Y. Hao, T. Han, Y. Cheng, A cooperative message authentication protocol in VANETs, in: 2012 IEEE Glob. Commun. Conf., IEEE, Anaheim, CA, USA, 2012, pp. 5562–5566. http://dx.doi.org/10.1109/GLOCOM.2012.6504006.

[103] N.B. Bhavesh, S. Maity, R.C. Hansdah, A protocol for authentication with multiple levels of anonymity (AMLA) in VANETs, in: 2013 27th Int. Conf. Adv. Inf. Netw. Appl. Work, IEEE, Barcelona, Spain, 2013, pp. 462–469. http://dx.doi.org/10.1109/WAINA.2013.4.

[104] S.-J. Horng, S.-F. Tzeng, Y. Pan, P. Fan, X. Wang, T. Li, M.K. Khan, b-SPECS+: Batch verification for secure pseudonymous authentication in VANET, IEEE Trans. Inf. Forensics Secur. 8 (2013) 1860–1875. http://dx.doi.org/10.1109/TIFS.2013.2277471.

[105] Xiaodong Lin, Xu. Li, Achieving efficient cooperative message authentication in vehicular ad hoc networks, IEEE Trans. Veh. Technol. 62 (2013) 3339–3348. http://dx.doi.org/10.1109/TVT.2013.2257188.

[106] W. Shen, L. Liu, X. Cao, Y. Hao, Y. Cheng, Cooperative message authentication in vehicular cyber-physical systems, IEEE Trans. Emerg. Top. Comput. 1 (2013) 84–97. http://dx.doi.org/10.1109/TETC.2013.2273221.

[107] M.-C. Chuang, J.-F. Lee, Team: trust-extended authentication mechanism for vehicular ad hoc networks, IEEE Syst. J. 8 (2014) 749–758. http://dx.doi.org/10.1109/JSYST.2012.2231792.

[108] X. Zhu, S. Jiang, L. Wang, H. Li, Efficient privacy-preserving authentication for vehicular ad hoc networks, IEEE Trans. Veh. Technol. 63 (2014) 907–919. http://dx.doi.org/10.1109/TVT.2013.2294032.

[109] P. Caballero-Gil, Security issues in vehicular ad hoc networks, in: Mob. Ad-Hoc Networks Appl., INTECH, 2016, pp. 67–88. http://cdn.intechopen.com/pdfs-wm/12879.pdf.

[110] A. Studer, F. Bai, B. Bellur, A. Perrig, Flexible, extensible, and efficient VANET authentication, J. Commun. Netw. 11 (2009) 574–588. http://dx.doi.org/10.1109/JCN.2009.6388411.

[111] L. He, W.T. Zhu, Mitigating DoS attacks against signature-based authentication in VANETs, in: 2012 IEEE Int. Conf. Comput. Sci. Autom. Eng, IEEE, Zhangjiajie, China, 2012, pp. 261–265. http://dx.doi.org/10.1109/CSAE.2012.6272951.

[112] R. Engoulou, Sécurisation des VANETS par la méthode de réputation des noeuds, Ecole Polytechnique de Montreal, 2013. https://publications.polymtl.ca/1100/. (Accessed 28 June 2017).

[113] J. Blum, A. Eskandarian, The threat of intelligent collisions, IT Prof. 6 (2004) 24–29. http://dx.doi.org/10.1109/MITP.2004.1265539.

[114] M. Raya, A. Aziz, J.-P. Hubaux, Efficient secure aggregation in VANETs, in: Proc. 3rd Int. Work. Veh. Ad Hoc Networks - VANET '06, ACM Press, New York, New York, USA, 2006, pp. 67–75. http://dx.doi.org/10.1145/1161064.1161076.

[115] European Telecommunications Standards Institute, Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA), Intell. Transp. Syst. 1.1.1 (2010) 1–86.

[116] V. Veque, C. Johnen, Hiérarchisation dans les réseaux ad hoc de véhicules, 8èmes Journées Francoph. Mobilité Ubiquité, UBIMOB. (2012) 45–52. https://hal.archives-ouvertes.fr/hal-00781267.

[117] R. Rajadurai, N. Jayalakshmi, Vehicular network: Properties, structure, challenges, attacks, solutions for improving scalability and security, Int. J Adv. Res. 1 (2013) 41–50. http://www.ijoar.org/journals/IJOARCS/papers/IJOARCS58.pdf.

[118] M. Raya, J.-P. Hubaux, The security of vehicular ad hoc networks, in: Proc. 3rd ACM Work. Secur. Ad Hoc Sens. Networks - SASN '05, ACM Press, New York, New York, USA, 2005, p. 11. http://dx.doi.org/10.1145/1102219.1102223.

[119] D. Singelee, B. Preneel, Location verification using secure distance bounding protocols, in: IEEE Int. Conf. Mob. Adhoc Sens. Syst. Conf. 2005, IEEE, 2005, pp. 834–840. http://dx.doi.org/10.1109/MAHSS.2005.1542879.

[120] Xiaodong Lin, Xiaoting Sun, Pin-Han Ho, Xuemin Shen, GSIS: A secure and privacy-preserving protocol for vehicular communications, IEEE Trans. Veh. Technol. 56 (2007) 3442–3456. http://dx.doi.org/10.1109/TVT.2007.906878.

[121] X. Lin, X. Sun, X. Wang, C. Zhang, P.-H. Ho, X. Shen, TSVC: timed efficient and secure vehicular communications with privacy preserving, IEEE Trans. Wirel. Commun. 7 (2008) 4987–4998. http://dx.doi.org/10.1109/T-WC.2008.070773.

[122] S.S. Manvi, M.S. Kakkasageri, D.G. Adiga, Message authentication in vehicular ad hoc networks: ECDSA based approach, in: 2009 Int. Conf. Futur. Comput. Commun., IEEE, 2009, pp. 16–20. http://dx.doi.org/10.1109/ICFCC.2009.120.

[123] T.W. Chim, S.M. Yiu, L.C.K. Hui, V.O.K. Li, Security and privacy issues for inter-vehicle communications in VANETs, in: 2009 6th IEEE Annu. Commun. Soc. Conf. Sensor, Mesh Ad Hoc Commun. Networks Work, IEEE, 2009, pp. 1–3. http://dx.doi.org/10.1109/SAHCNW.2009.5172962.

[124] J. Sun, C. Zhang, Y. Zhang, Y. Fang, An identity-based security system for user privacy in vehicular ad hoc networks, IEEE Trans. Parallel Distrib. Syst. 21 (2010) 1227–1239. http://dx.doi.org/10.1109/TPDS.2010.14.

[125] A. Wasef, X. Shen, Efficient group signature scheme supporting batch verification for securing vehicular networks, in: 2010 IEEE Int. Conf. Commun., IEEE, Cape Town, South Africa, 2010, pp. 1–5. http://dx.doi.org/10.1109/ICC.2010.5502136.

[126] Lei Zhang, Qianhong Wu, A. Solanas, J. Domingo-Ferrer, A scalable robust authentication protocol for secure vehicular communications, IEEE Trans. Veh. Technol. 59 (2010) 1606–1617. http://dx.doi.org/10.1109/TVT.2009.2038222.

[127] T.W. Chim, S.M. Yiu, L.C.K. Hui, Z.L. Jiang, V.O.K. Li, SPECS: Secure and privacy enhancing communications schemes for VANETs, in: Int. Conf. Ad Hoc Networks, Springer, Berlin, Heidelberg, 2010, pp. 160–175. http://dx.doi.org/10.1007/978-3-642-11723-7_11.

[128] J.-L. Huang, L.-Y. Yeh, H.-Y. Chien, ABAKA: An anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks, IEEE Trans. Veh. Technol. 60 (2011) 248–262. http://dx.doi.org/10.1109/TVT.2010.2089544.

[129] W.W. Rhim, A Study on MAC-Based Efficient Message Authentication Scheme for VANET, Hanyang University, 2012.

[130] H. Lu, J. Li, M. Guizani, A novel ID-based authentication framework with adaptive privacy preservation for VANETs, in: 2012 Comput. Commun. Appl. Conf., IEEE, Hong Kong, China, 2012, pp. 345–350. http://dx.doi.org/10.1109/ComComAp.2012.6154869.

[131] A. Wasef, X. Shen, EMAP: Expedite message authentication protocol for vehicular ad hoc networks, IEEE Trans. Mob. Comput. 12 (2013) 78–89. http://dx.doi.org/10.1109/TMC.2011.246.

[132] K. Ravi, S.A. Kulkarni, A secure message authentication scheme for VANET using ECDSA, in: 2013 Fourth Int. Conf. Comput. Commun. Netw. Technol., IEEE, 2013, pp. 1–6. http://dx.doi.org/10.1109/ICCCNT.2013.6726769.

[133] S. Taeho, J. Jaeyoon, K. Hyunsung, L. Sung-Woon, Enhanced MAC-based efficient message authentication scheme over VANET, in: 7th In- Ternational Multi-Conference Eng. Technol. Innov. USA, 2014, pp. 110–113.

[134] M.H. Jahanian, F. Amin, A.H. Jahangir, Analysis of TESLA protocol in vehicular ad hoc networks using timed colored Petri nets, in: 2015 6th Int. Conf. Inf. Commun. Syst, IEEE, Amman, Jordan, 2015, pp. 222–227. http://dx.doi.org/10.1109/IACS.2015.7103231.

[135] J. Li, H. Lu, M. Guizani, ACPN: A novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs, IEEE Trans. Parallel Distrib. Syst. 26 (2015) 938–948. http://dx.doi.org/10.1109/TPDS.2014.2308215.

[136] G. Guette, C. Bryce, Using TPMs to secure vehicular ad-hoc networks (VANETs), in: Inf. Secur. Theory Pract. Smart Devices, Converg. Next Gener. Networks, Springer, Berlin, Heidelberg, 2008, pp. 106–116. http://dx.doi.org/10.1007/978-3-540-79966-5_8.

[137] R. Mishra, S. Singh, A. Singh, Session seizure: Hijacking, in: Proc. Natl. Conf. Contemp. Comput. Informatics, 2015: pp. 227–229. https://books.google.com/books/about/Proceedings_of_National_Conference_on_Co.html?id=r3OmjwEACAAJ. (Accessed 29 June 2017).

[138] A. Rao, A. Sangwan, A.A. Kherani, A. Varghese, B. Bellur, R. Shorey, Secure V2V communication with certificate revocations, in: 2007 Mob. Netw. Veh. Environ, IEEE, 2007, pp. 127–132. http://dx.doi.org/10.1109/MOVE.2007.4300817.

[139] B. Aslam, C. Zou, Distributed certificate and application architecture for VANETs, in: MILCOM 2009 - 2009 IEEE Mil. Commun. Conf., IEEE, 2009, pp. 1–7. http://dx.doi.org/10.1109/MILCOM.2009.5379867.

[140] A.M. Malla, R.K. Sahu, Security attacks with an effective solution for DOS attacks in VANET, Int. J. Comput. Appl. 66 (2013) 45–49. http://dx.doi.org/10.5120/11252-6467.

[141] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, A. Hassan, Vehicular ad hoc networks (VANETS): status, results, and challenges, Telecommun. Syst. 50 (2012) 217–241. http://dx.doi.org/10.1007/s11235-010-9400-5.

[142] K. Verma, H. Hasbullah, A. Kumar, Prevention of DoS Attacks in VANET, Wirel. Pers. Commun. 73 (2013) 95–126. http://dx.doi.org/10.1007/s11277-013-1161-5.

[143] H. Hasrouny, C. Bassil, A.E. Samhat, A. Laouiti, Security Risk Analysis of a Trust Model for Secure Group Leader-Based Communication in VANET, Springer, Singapore, 2017, pp. 71–83. http://dx.doi.org/10.1007/978-981-10-3503-6_6.

[144] K. Plößl, H. Federrath, A privacy aware and efficient security infrastructure for vehicular ad hoc networks, Comput. Stand. Interfaces 30 (2008) 390–397. http://dx.doi.org/10.1016/j.csi.2008.03.007.

Please cite this article in press as: G. De La Torre, et al., Driverless vehicle security: Challenges and future research opportunities, Future Generation Computer Systems (2018), https://doi.org/10.1016/j.future.2017.12.041.

[145] M. Abuelela, S. Olariu, K. Ibrahim, A secure and privacy aware data dissemination for the notification of traffic incidents, in: VTC Spring 2009 - IEEE 69th Veh. Technol. Conf., IEEE, 2009, pp. 1–5. http://dx.doi.org/10.1109/VETECS.2009.5073340.

[146] W. Whyte, A. Weimerskirch, V. Kumar, T. Hehn, A security credential management system for V2V communications, in: 2013 IEEE Veh. Netw. Conf., IEEE, 2013, pp. 1–8. http://dx.doi.org/10.1109/VNC.2013.6737583.

[147] C.D. Jung, C. Sur, Y. Park, K.-H. Rhee, A robust conditional privacy-preserving authentication protocol in vanet, in: Secur. Priv. Mob. Inf. Commun. Syst. Lect. Notes Inst. Comput. Sci. Soc. Informatics Telecommun. Eng. vol. 17, Springer Berlin Heidelberg, ISBN: 978-3-642-04433-5, 2009, p. 35. http://dx.doi.org/10.1007/978-3-642-04434-2_4.

[148] F.M. Salem, M.H. Ibrahim, I.I. Ibrahim, Non-interactive authentication scheme providing privacy among drivers in vehicle-to-vehicle networks, in: 2010 Sixth Int. Conf. Netw. Serv., IEEE, 2010, pp. 156–161. http://dx.doi.org/10.1109/ICNS.2010.28.

[149] European Telecommunications Standards Institute, Intelligent Transport Systems (ITS); Security; Trust and Privacy Management, Intell. Transp. Syst. 1.1.1 (2012) 1–30.

[150] J. Newsome, E. Shi, D. Song, A. Perrig, The sybil attack in sensor networks: Analysis & defenses, in: Proc. 3rd Int. Symp. Inf. Process. Sens. Netw., IEEE, Berkeley, CA, USA, 2004, pp. 359–368.

[151] B. Xiao, B. Yu, C. Gao, Detection and localization of sybil nodes in vanets, in: Proc. 2006 Work. Dependability Issues Wirel. Ad Hoc Networks Sens. Networks - DIWANS '06, ACM Press, New York, New York, USA, 2006, pp. 1–8. http://dx.doi.org/10.1145/1160972.1160974.

[152] T. Zhou, R.R. Choudhury, P. Ning, K. Chakrabarty, P2DAP — Sybil attacks detection in vehicular ad hoc networks, IEEE J. Sel. Areas Commun. 29 (2011) 582–594. http://dx.doi.org/10.1109/JSAC.2011.110308.

[153] P. Fan, J.G. Haran, J. Dillenburg, P.C. Nelson, Cluster-Based framework in vehicular ad-hoc networks, in: Ad-Hoc, Mobile, Wirel. Netw., Springer, Berlin, Heidelberg, 2005, pp. 32–42. http://dx.doi.org/10.1007/11561354_5.

[154] R. Van Der Heijden, Security Architectures in V2V and V2I Communication, 2010.

[155] G. Samara, W.A.H. Al-Salihy, R. Sures, Security analysis of vehicular ad hoc nerworks (VANET), in: 2010 Second Int. Conf. Netw. Appl. Protoc. Serv., IEEE, 2010, pp. 55–60. http://dx.doi.org/10.1109/NETAPPS.2010.17.

[156] G. Karagiannis, O. Altintas, E. Ekici, G. Heijenk, B. Jarupan, K. Lin, T. Weil, Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions, IEEE Commun. Surv. Tutor. 13 (2011) 584–616. http://dx.doi.org/10.1109/SURV.2011.061411.00019.

[157] L. Song, Q. Han, J. Liu, Investigate key management and authentication models in VANETs, in: 2011 Int. Conf. Electron. Commun. Control, IEEE, 2011, pp. 1516–1519. http://dx.doi.org/10.1109/ICECC.2011.6067807.

[158] M.S. Al-kahtani, Survey on security attacks in vehicular ad hoc networks, VANETs, in: 2012 6th Int. Conf. Signal Process. Commun. Syst., IEEE, 2012, pp. 1–9. http://dx.doi.org/10.1109/ICSPCS.2012.6507953.

[159] R. Shringar Raw, M. Kumar, N. Singh, Security challenges, issues and their solutions for vanet, Int. J. Netw. Secur. Its Appl. 5 (2013) 95–105. http://dx.doi.org/10.5121/ijnsa.2013.5508.

[160] R.G. Engoulou, M. Bellache, S. Pierre, A. Quintero, VANET security surveys, Comput. Commun. 44 (2014) 1–13. http://dx.doi.org/10.1016/j.comcom.2014.02.020.

[161] R. Raiya, S. Gandhi, Survey of various security techniques in VANET, Int. J. Adv. Res. Comput. Sci. Softw. Eng. 4 (2014) 431–433.

[162] V. Hoa La, A. Cavalli, Security attacks and solutions in vehicular ad hoc networks: A survey, Int. J. AdHoc Netw. Syst. 4 (2014) 1–20. http://dx.doi.org/10.5121/ijans.2014.4201.

[163] N.J. Patel, R.H. Jhaveri, Trust based approaches for secure routing in VANET: A survey, Proc. Comput. Sci. 45 (2015) 592–601. http://dx.doi.org/10.1016/j.procs.2015.03.112.

[164] D. Kushwaha, P. Kumar Shukla, R. Baraskar, A survey on sybil attack in vehicular ad-hoc network, Int. J. Comput. Appl. 98 (2014) 31–36. http://dx.doi.org/10.5120/17262-7614.

[165] S. Jafarnejad, L. Codeca, W. Bronzi, R. Frank, T. Engel, A car hacking experiment: When connectivity meets vulnerability, in: 2015 IEEE Globecom Work. GC Wkshps 2015 - Proc., IEEE, San Diego, CA, USA, 2016 p. N/A, http://dx.doi.org/10.1109/GLOCOMW.2015.7413993.

[166] M.T. Garip, P. Reiher, M. Gerla, Ghost: Concealing vehicular botnet communication in the VANET control channel, in: 2016 Int. Wirel. Commun. Mob. Comput. Conf. IWCMC 2016, IEEE, Paphos, Cyprus, 2016, pp. 1–6. http://dx.doi.org/10.1109/IWCMC.2016.7577024.

[167] R. Sunnadkal, B. Soh, H. Phan, A four-stage design approach towards securing a vehicular ad hoc networks architecture, in: Proc. - 5th IEEE Int. Symp. Electron. Des. Test Appl. DELTA 2010, IEEE, Ho Chi Minh City, Vietnam, Vietnam, 2010. http://dx.doi.org/10.1109/DELTA.2010.49.

[168] T.W. Chim, S.M. Yiu, L.C.K. Hui, V.O.K. Li, VSPN: VANET-based secure and privacy-preserving navigation, IEEE Trans. Comput. 63 (2014) 510–524. http://dx.doi.org/10.1109/TC.2012.188.

[169] K.M.A. Alheeti, A. Gruebler, K.D. McDonald-Maier, An intrusion detection system against malicious attacks on the communication network of driverless cars, in: 2015 12th Annu. IEEE Consum. Commun. Netw. Conf. CCNC 2015, IEEE, Las Vegas, NV, USA, 2015. http://dx.doi.org/10.1109/CCNC.2015.7158098.

[170] K.M.A. Alheeti, K.D. McDonald-Maier, Hybrid intrusion detection in connected self-driving vehicles, in: 2016 22nd Int. Conf. Autom. Comput. ICAC 2016 Tackling New Challenges Autom. Comput, IEEE, Colchester, UK, 2016 p. N/A, http://dx.doi.org/10.1109/IConAC.2016.7604962.

[171] O. Henniger, L. Apvrille, A. Fuchs, Y. Roudier, A. Ruddle, B. Weyl, Security requirements for automotive on-board networks, in: 2009 9th Int. Conf. Intell. Transp. Syst. Telecommun. ITST 2009, IEEE, Lille, France, 2009, pp. 641–646. http://dx.doi.org/10.1109/ITST.2009.5399279.

[172] W. Zeng, M.A.S. Khalid, S. Chowdhury, In-vehicle networks outlook: Achievements and challenges, IEEE Commun. Surv. Tutor. 18 (2016) 1552–1571. http://dx.doi.org/10.1109/COMST.2016.2521642.

[173] I. Studnia, V. Nicomette, E. Alata, Y. Deswarte, M. Kaaniche, Y. Laarouchi, Survey on security threats and protection mechanisms in embedded automotive networks, in: 2013 43rd Annu. IEEE/IFIP Conf. Dependable Syst. Networks Work, IEEE, Budapest, 2013, pp. 1–12. http://dx.doi.org/10.1109/DSNW.2013.6615528.

[174] S. Tuohy, M. Glavin, C. Hughes, E. Jones, M. Trivedi, L. Kilmartin, Intra-Vehicle networks: A review, IEEE Trans. Intell. Transp. Syst. 16 (2015) 534–545. http://dx.doi.org/10.1109/TITS.2014.2320605.

[175] FlexRay Automotive Communication Bus Overview, 2016. http://www.ni.com/white-paper/3352/en/ (Accessed 6 July 2017).

[176] R. Cummings, Easing the Transition of System Designs from CAN To FlexRay, SAE Tech. Pap, 2008. http://dx.doi.org/10.4271/2008-01-0804.

[177] C.P. Quigley, R. McMurran, R.P. Jones, P.T. Faithfull, An investigation into cost modelling for design of distributed automotive electrical architectures, in: 2007 3rd Inst. Eng. Technol. Conf. Automot. Electron, IEEE Xplore, Warwick, UK, 2007.

[178] FlexRay, Ethernet vie for role as safety systems share data - SAE International, SAE Int. 2014. http://articles.sae.org/12862/. (Accessed 6 July 2017).

[179] FlexRay Consortium, FlexRay communications system protocol specification version 3.0.1, October 2010, pp. 1–341. http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:FlexRay+Communications+System+Protocol+Specification#0.

[180] X. He, Q. Wang, Z. Zhang, A survey of study of flexray systems for automotive net, in: Proc. 2011 Int. Conf. Electron. Mech. Eng. Inf. Technol., IEEE, Harbin, Heilongjiang, China, 2011, pp. 1197–1204. http://dx.doi.org/10.1109/EMEIT.2011.6023309.

[181] G. Han, H. Zeng, Y. Li, W. Dou, SAFE: Security-aware flexray scheduling engine, in: Des. Autom. Test Eur. Conf. Exhib. (DATE), 2014, IEEE Conference Publications, Dresden, Germany, 2014, pp. 1–4. http://dx.doi.org/10.7873/DATE.2014.021.

[182] B. Groza, S. Murvay, A. van Herrewege, I. Verbauwhede, LiBrA-CAN: A lightweight broadcast authentication protocol for controller area networks, in: Cryptol. Netw. Secur., 2012, pp. 185–200. http://dx.doi.org/10.1007/978-3-642-35404-5_15.

[183] A. Van Herrewege, D. Singelee, I. Verbauwhede, CANAuth - A Simple, Backward Compatible Broadcast Authentication Protocol for CAN bus, ECRYPT Work. Light. Cryptogr. 2011, pp. 299–235. http://www.uclouvain.be/crypto/ecrypt_lc11/static/post_proceedings.pdf.

[184] O. Hartkopp, C. Reuber, R. Schilling, Macan-message authenticated can, in: Proc. 10th Int. Conf. Embed. Secur. Cars, Berlin, Germany, 2012.

[185] M. Wolf, T. Gendrullis, Design, implementation, and evaluation of a vehicular hardware security module, in: Inf. Secur. Cryptol. - ICISC 2011, Springer, Berlin, Heidelberg, Seoul, South Korea, 2012, pp. 302–318. http://dx.doi.org/10.1007/978-3-642-31912-9_20.

[186] H. Schweppe, Y. Roudier, B. Weyl, L. Apvrille, D. Scheuermann, Car2X communication: Securing the last meter - A cost-effective approach for ensuring trust in Car2X applications using in-vehicle symmetric cryptography, in: 2011 IEEE Veh. Technol. Conf. (VTC Fall), IEEE, San Francisco, CA, USA, 2011, pp. 1–5. http://dx.doi.org/10.1109/VETECF.2011.6093081.

[187] C.-W. Lin, A. Sangiovanni-Vincentelli, Cyber-security for the controller area network (can) communication protocol, in: 2012 Int. Conf. Cyber Secur., IEEE, Washington, DC, USA, 2012, pp. 1–7. http://dx.doi.org/10.1109/CyberSecurity.2012.7.

[188] I. Broster, A. Burns, An analysable bus-guardian for event-triggered communication, in: Proc. 24th IEEE Int. Real-Time Syst. Symp., IEEE Computer Society Press, Washington, DC, USA, 2003, p. 410 http://dl.acm.org/citation.cfm?id=956589 (Accessed 6 July 2017).

[189] H. Schweppe, Y. Roudier, Security and privacy for in-vehicle networks, in: 2012 IEEE 1st Int. Work. Veh. Commun. Sensing, Comput., IEEE, Seoul, South Korea, 2012, pp. 12–17. http://dx.doi.org/10.1109/VCSC.2012.6281235.

[190] M. Muter, A. Groll, F.C. Freiling, A structured approach to anomaly detection for in-vehicle networks, in: 2010 Sixth Int. Conf. Inf. Assur. Secur., IEEE,

Atlanta, GA, USA, 2010, pp. 92–98. http://dx.doi.org/10.1109/ISIAS.2010.5604050.
[191] M. Muter, N. Asaj, Entropy-based anomaly detection for in-vehicle networks, in: 2011 IEEE Intell. Veh. Symp., IEEE, Baden-Baden, Germany, 2011, pp. 1110–1115. http://dx.doi.org/10.1109/IVS.2011.5940552.
[192] W.A. Arbaugh, D.J. Farber, J.M. Smith, A secure and reliable bootstrap architecture, in: 1997 IEEE Symp. Secur. Priv. Proc., IEEE Comput. Soc. Press, Oakland, CA, USA, 1997, pp. 65–71. http://dx.doi.org/10.1109/SECPRI.1997.601317.
[193] L. Pan, X. Zheng, H.X. Chen, T. Luan, H. Bootwala, L. Batten, Cyber security attacks to modern vehicular systems, J. Inf. Secur. Appl. 36 (2017) 90–100. http://dx.doi.org/10.1016/J.JISA.2017.08.005.
[194] A. Grzemba, MOST The Automotive Multimedia Network, fromMOST25 to MOST150, Franzis Verlag GmbH, 2011.
[195] MOST Informative, 2014.
[196] G. Grispos, W.B. Glisson, K.-K.R. Choo, Medical cyber-physical systems development: A forensics-driven approach, in: 2017 IEEE/ACM Int. Conf. Connect. Heal. Appl. Syst. Eng. Technol., IEEE, 2017, pp. 108–113. http://dx.doi.org/10.1109/CHASE.2017.68.
[197] M. Conti, A. Dehghantanha, K. Franke, S. Watson, Internet of Things security and forensics: Challenges and opportunities, Future Gener. Comput. Syst. 78 (2) (2018) 544–546.
[198] D. Jacobs, K.-K.R. Choo, M.T. Kechadi, N.-A. Le-Khac, Volkswagen car entertainment system forensics, in: Proceedings of The 16th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, IEEE TrustCom 2017, 2017, pp. 699–705.
[199] S. Watson, A. Dehghantanha, Digital forensics: the missing piece of the Internet of Things promise, Comput. Fraud Secur. 2016 (6) (2016) 5–8.
[200] L. Wang, Y. Ma, A.Y. Zomaya, R. Ranjan, D. Chen, A parallel file system with application-aware data layout policies for massive remote sensing image processing in digital earth, IEEE Trans. Parallel Distrib. Syst. 26 (2015) 1497–1508. http://dx.doi.org/10.1109/TPDS.2014.2322362.
[201] M. Villari, M. Fazio, S. Dustdar, O. Rana, R. Ranjan, Osmotic computing: A new paradigm for edge/cloud integration, IEEE Cloud Comput. 3 (2016) 76–83. http://dx.doi.org/10.1109/MCC.2016.124.
[202] A. Khoshkbarforoushha, R. Ranjan, R. Gaire, E. Abbasnejad, L. Wang, A.Y. Zomaya, Distribution based workload modelling of continuous queries in clouds, IEEE Trans. Emerg. Top. Comput. 5 (2017) 120–133. http://dx.doi.org/10.1109/TETC.2016.2597546.
[203] A. Khoshkbarforoushhaab, A. Khosravianc, R. Ranjan, Elasticity management of streaming data analytics flows on clouds, J. Comput. System Sci. 89 (2017) 24–40. http://dx.doi.org/10.1016/J.JCSS.2016.11.002.
[204] N.H. Ab Rahman, N.D.W. Cahyani, K.-K.R. Choo, Cloud incident handling and forensic-by-design: cloud storage as a case study, Concurr. Comput. Pract. Exp. 29 (2017) e3868. http://dx.doi.org/10.1002/cpe.3868.
[205] N.H. Ab Rahman, W.B. Glisson, Y. Yang, K.-K.R. Choo, Forensic-by-design framework for cyber-physical cloud systems, IEEE Cloud Comput. 3 (2016) 50–59. http://dx.doi.org/10.1109/MCC.2016.5.
[206] C. Huang, R. Lu, K.-K.R. Choo, Vehicular fog computing: Architecture, use case and security and forensic challenges, IEEE Commun. Mag. 55 (11) (2017) 105–111. http://dx.doi.org/10.1109/MCOM.2017.1700322.
[207] C. Lin, D. He, N. Kumar, K.-K.R. Choo, A. Vinel, X. Huang, Security and privacy for internet of drones: Challenges and solutions, IEEE Commun. Mag. (2018) in press.

Gonzalo De La Torre Parra received the B.S. in Electrical Engineering from Texas A&M University-Kingsville, USA, in 2009 and the M.S. in Electrical Engineering (Telecommunications Concentration) from The University of Texas at San Antonio, USA, in 2015. He is currently pursuing the Ph.D. in Electrical Engineering at The University of Texas at San Antonio. His current research is focused on the development of Deep Learning Algorithms on Network Security. From 2015 to 2017, he has been a developer of Chameleon Cloud, an NSF sponsored cloud infrastructure, has held the Co-Chair position of OpenStack's Cloud Application Hack Work Group, and manages research projects focused on cloud, networks, and security at the Open Cloud Institute. Mr. De La Torre Parra's awards and honors include the 2nd Place Award on SHPE's Extreme Engineering National STEM Competition (2013), the 2nd Place Award on HENAAC's XIV National STEM Competition (2013), the San Antonio Mexican Foundation for Education (SAMFE) award (2013), CONACYT's Master's Degree Fellowship (2013), NSF-Open Cloud Institute Fellowship (2016), and CONACYT's Ph.D. Degree Fellowship (2017).

Paul Rad is cofounder and assistant director of Open Cloud Institute (OCI), and associate professor at The University of Texas at San Antonio, USA. His research interests include artificial intelligence and machine learning, cyber analytics, and cloud computing with applications to cyber–physical systems and IoT, machine sensing, and decentralized decision making and trust. He received Ph.D. degree in Electrical and Computer Engineering on Cyber Analytics from the University of Texas at San Antonio. He holds fourteen US patents on Cyber Infrastructure, Cloud Computing, and Big Data Analytics. Rad has advised over 200+companies on cloud computing and data analytics with over 50 keynote presentations.

Kim-Kwang Raymond Choo received the Ph.D. degree in information security from the Queensland University of Technology, Australia, in 2006. He currently holds the Cloud Technology Endowed professorship with The University of Texas. He serves on the editorial board of Cluster Computing, Digital Investigation, IEEE Access, IEEE Cloud Computing, IEEE Communications Magazine, Future Generation Computer Systems, Journal of Network and Computer Applications, PLoS ONE, etc. He also serves as the Special Issue Guest Editor of ACM Transactions on Embedded Computing Systems (2017), ACM Transactions on Internet Technology (2016), Computers & Electrical Engineering (2017), Digital Investigation (2016), Future Generation Computer Systems (2016), IEEE Cloud Computing (2015), IEEE Network (2016), IEEE Transactions on Dependable and Secure Computing (2017), Journal of Computer and System Sciences (2017), Multimedia Tools and Applications (2017), Personal and Ubiquitous Computing (2017), Pervasive and Mobile Computing (2016), Wireless Personal Communications (2017), etc. He was named one of 10 Emerging Leaders in the Innovation category of The Weekend Australian Magazine/Microsoft's Next 100 series, and Cybersecurity Educator of the Year — APAC (produced in cooperation with the Information Security Community on LinkedIn) in 2009 and 2016, respectively. He and his team won Germany's University of Erlangen-Nuremberg (FAU) Digital Forensics Research Challenge 2015. He is the recipient of ESORICS 2015 Best Research Paper Award, Highly Commended Award by Australia New Zealand Policing Advisory Agency, Fulbright Scholarship in 2009, 2008 Australia Day Achievement Medallion, the British Computer Society's Wilkes Award for the best (sole-authored) paper published in the 2007 volume of The Computer Journal, and ACISP 2005 Best Student Paper Award. He is also a Fellow of the Australian Computer Society, an IEEE Senior Member, and an Honorary Commander of the 502nd Air Base Wing at Joint Base San Antonio-Fort Sam Houston, USA.

Please cite this article in press as: G. De La Torre, et al., Driverless vehicle security: Challenges and future research opportunities, Future Generation Computer Systems (2018), https://doi.org/10.1016/j.future.2017.12.041.