Addressing Malware Attacks on Connected and Autonomous Vehicles: Recent Techniques and Challenges

Aiman Al-Sabaawi, Khamael Al-Dulaimi, Ernest Foo and Mamoun Alazab

Abstract Part of the wider development and monitoring of smart environments for an intelligent cities approach is the building of an intelligent transportation system. Such a system involves the development of modern vehicles which significantly improve passenger safety and comfort, a trend that is expected to increase in the coming years. There are key factors relating to safety impacts and security vulnerabilities that may emerge during the increased deployment of automated vehicles and the security and privacy of connected and automated vehicle systems. They include ways of defining the security of malware-relevant system boundaries including electronic control units, silicon hardware, software, vehicle systems, infrastructure, network connectivity and more. In addition, vehicle industries are facing many problems with critical security and privacy issues, influenced by the smart environments for an intelligent cities approach. Such problems are related to hardware and software applications that allow the interfacing of Vehicle to Vehicle (V2V) and Vehicle to Infrastructure networks (V2I). In this chapter, we present connected car methods relating to the attack, defence and detection of malware in vehicles. Critical issues are introduced regarding the sharing of safety information and the verification of the integrity of

Aiman Al-Sabaawi
Queensland University of Technology, Queensland, Australia,
Department of Computer Science, Al-Nahrain University, Baghdad, Iraq , e-mail: a.alsabaawi@connect.qut.edu.au

Khamael Al-Dulaimi
Queensland University of Technology, Queensland, Australia,
Department of Computer Science, Al-Nahrain University, Baghdad, Iraq,
e-mail: khamaelabbaskhudhair.aldulaimi@hdr.qut.edu.au

Ernest Foo
of Information and Communication Technology, Griffith University, Queensland, Australia, e-mail: e.foo@griffith.edu.au

Mamoun Alazab
College of Engineering, Information Technology and Environment, Charles Darwin University, Northern Australia, Australia, e-mail: alazab.m@ieee.org

this information from Vehicle to Vehicle and Vehicle to Infrastructure networks. In particular, we discuss the challenges and review state-of-the-art intra-inter vehicle communication. Hackers can access this information in V2V/V2I networks and broadcast fake messages and malware to break the security system by using weak points in vehicles and networks. We present important security approaches that are used in vehicles which can fully protect the vehicle security architecture by detecting the attempts made and the methods used by hackers to tackle malware and security problems in vehicles. We present a comprehensive overview of current research on advanced intra-inter vehicle communication networks and identify outstanding research questions that may be used to achieve high levels of vehicle security and privacy in intelligent cities in the future.

1 Introduction

Smart city or smart building technology has been advancing in recent years due to the development of communication technologies and wiring which are associated with the fields of power, health, education, industries and transportation. Buildings are becoming more complex, with interconnected Internet of Things (IoT) systems offering technological equipment and cost-efficient buildings and energy. The infrastructure of the IoT is still developing and offers many benefits for humans including monitoring asset movements, turning lights on/off as needed, optimizing room occupancy, air conditioning systems, health systems, vehicular and road connected systems, security systems (monitoring camera systems) and location systems [48, 37].

The IoT enables cities to grow and expand. Officials in cities with the technology of the IoT can access valuable data to gain a better understanding of their city's operations. Those data enable the control of traffic, the empowerment of local law enforcement, allow improved security of connected vehicles, monitoring of the environment and enable city-wide connectivity and tracking of parking efficiency. These cities play a significant role in fostering creativity and innovation. The creation of customized IoT applications positions cities at the technological forefront which, in turn, attracts new residents and businesses. Intelligent transportation systems, monitoring the way people commute in metros and smart cities, are one benefit. An intelligent transportation system offers a novel approach to the provision of different transportation modes, advanced infrastructure and traffic and mobility management solutions. It uses a number of electronic, sensor, wireless and communication technologies to provide consumers with access to a smarter, safer, and faster way of travelling [48, 37].

1.1 Important Technologies in Intelligent Transportation System in Smart Cities

1. Advanced Tracking System: modern vehicles are connected with in-vehicle GPS. The GPS system can offer two-way communication, helping traffic professionals to locate vehicles, check speeding vehicles, and provide emergency services. Smartphones, mobile applications and Google maps have become useful tools in tracking, understanding road quality, traffic density and locating different routes and places.
2. Advanced Sensing Technologies: These include intelligent sensors both in vehicles and road infrastructure. Radio Frequency Identification (RFI) and intelligent beacon sensing technologies are ensuring the safety of drivers in cities worldwide. Road reflectors and inductive loops are built into roads, assisting with traffic control and safe driving, especially at night. They can also provide information about vehicle density at particular times and can identify vehicles at both slow and high speeds.
3. Advanced Video Vehicle Detection: Video cameras or CCTV surveillance can solve many problems for traffic managers. Video footage of strategic places and prime junctions can help operators observe traffic flow and identify any emergency situation or road congestion. In-built vehicle sensors and automatic number plate detection help to check vehicles for security purposes.
4. Advanced Traffic Light Systems: Radio Frequency Identification (RFID) is used in traffic light systems. This technology can offer correct algorithms and databases even when applied to multiple lanes, road junctions and vehicles. These lights can adjust themselves during critical and peak hour traffic situations without any human presence.
5. Emergency E-Call Vehicle Service: During an emergency situation such as an accident or mishap, in-vehicle sensors can establish contact with a nearby emergency centre. An e-call will help a driver to connect to a trained operator and also transmit important information such as time, location, direction of vehicle and vehicle identification directly to the centre [37].

1.2 Benefits of Intelligent Transportation System

1. Minimizing Pollution: An intelligent transportation system aims to promote the use of public transport by the general public. If it provides single point services and access to real-time information about the transport schedule, people will prefer to use an intelligent transportation system and reduce private vehicle usage, thereby lowering traffic congestion and lowering pollution levels.
2. Security and Safety: Advanced sensing technologies help to provide emergency and critical care services to drivers and people when required, such as real-time data analysis, including CCTV, GPS, internet connectivity and wireless and virus and malware detection [11]. Surveillance of public transportation also helps to

alert city managers to the risk of terror elements and to avoid mishaps or terror attacks.
3. Market for Mobile Applications: Recently, modern transportation has come to depend more on smartphones and mobile applications to identify parking spots, route guides, destination points, weather forecasts and arrival and departure details.
4. Smart Parking Solutions: Smart parking solutions, combined with appropriate infrastructure, internet connectivity and security cameras, can minimize parking problems. Many urban areas now have multi-layer parking systems. There are also many applications which provide users with information about free parking spaces available nearby [37].

1.3 Challenges of Intelligent Transportation System

To support these benefits and sophisticated features in an intelligent transportation system, modern vehicles are developed using software, an assortment of embedded computing devices, sensors, communication interfaces and actuators. However, these lead to many challenges that affect human life and safety [22].

Vehicle industries predict that as the cost of software and electronics fall, security-related incidents will become a serious threat. Exploiting vulnerabilities in the vehicle's electronics may allow the remote control of vehicle components. An attacker can turn off the vehicle's lights or even control the brakes while on the move [29]. More recently, attacks on production vehicles, for example, exploiting vulnerabilities in Fiat/Chrysler's Uconnect system, enabled hackers to control the vehicles, turning off the engine and controlling the steering over the Internet [23, 48], with the company urging owners to update their vehicles' software to patch the identified vulnerabilities [48].

Moreover, many of the enhanced services of these modern inter-connected vehicles rely on the location of the vehicles and their drivers, information that, by its nature, gives rise to significant privacy concerns. Securing the various heterogeneous hardware and software platforms and networks in the intelligent transformation system ecosystem is still a challenging task. While security is an important key in various aspects of smart vehicle related Information and Communications Technology (ICT) deployments, many aspects of efficient intelligent transportation operations have safety issues and other Quality of Service (QoS) characteristics which may limit the applicability of complex security initiatives. Therefore, potential solutions should be considered for these limitations by identifying attack type, defence and detection [22].

Given the advantages of a connected vehicle, security in vehicle networks and their characteristics and issues, it is crucial to understand how current intelligent transportation systems can be adapted to work with smart environments for intelligent cities. In this chapter, we provide an overview of connected vehicle methods in intra-inter vehicle communication. We then provide a survey of the recent history of

three key features in vehicle security and malware: attack, defence and detection. There has been extensive research in each area and many studies address intra-inter vehicle communication, which is a critical problem in vehicle technology. The following review critically describes the literature regarding the identification of attacks such malware and their types and the defences and solutions in intra-inter vehicle communication. The detection issues and challenges for each type of communication will be presented. The literature also includes the recent techniques and their challenges and issues regarding vehicle security from malware including attacks, defences and detection in intra-inter communication networks. The objective of this chapter is to help researchers to address these challenges in future work and in the further investigation of attacks, defences and detection, as well as to make significant changes to the design of vehicle systems to improve automotive security and prevent any malware and cyber terrorists from attacking vehicles.

This chapter is organized as follows: the first section presents a comprehensive overview of the vehicle connected methods, including attacks, detection and defence. In the second section, recent techniques and their challenges are discussed. The third section comprises the conclusion of the chapter.

2 Literature Review

Because modern technology has introduced more intelligence and complexity into the car industry, researchers are required to take greater responsibility for both safety and security. Vehicle security is different from vehicle safety, which includes vehicle speed [9] and vehicle integrated design [20]. Vehicle security, however, is essential to delivering vehicle safety from malware [44]. With a connected environment, vehicles, infrastructure, and pedestrians can exchange information, either through a peer-to-peer connectivity protocol or a centralized system via a 4G or more advanced telecommunication and security network. This technology has the potential to be one of the most disruptive technologies for urban and smart cities. The interaction and exchange of information regarding the use of malware may occur in vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), pedestrian-to-infrastructure (P2I), or vehicle-to-pedestrian applications (V2P) [51].

Vehicle security covers many aspects including Immobilizers, Car-to-Car communication, Car-to-infrastructure communication, Car-to-X communications, Cloud and Smartphone or smart device [12]. Recently, security analysis has been investigated in vehicle production and it was discovered that there are many reasons for security development. By accessing the in-vehicle 3G or Bluetooth, an attacker may tamper with the brakes while people are driving cars. In addition, car thieves have the ability to exploit security breaches in keyless-entry systems or to generate spare keys by using the on-board diagnostic system or using malware. Today, the weakness of security measures in vehicles can cause many financial problems, such as decreasing mileage to extend warranty claims by illegal chip adjusting [47]. Connected car methods are shown in Figure-1.

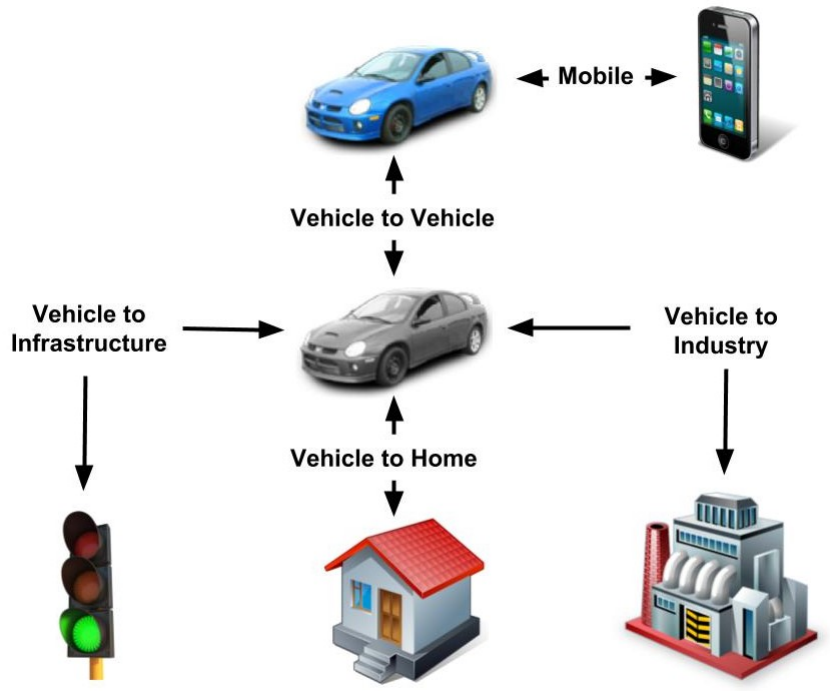

Fig. 1 The concept of the connected car.

1. Car-to-Car communication: This term refers to inter-vehicle communication exchange between two cars, for example, to warn others of a change in the road surface, obstacles on the roadway, or other dangers.
2. Car-to-infrastructure communication: This refers to communication between cars and components of the infrastructure using wireless communication. Components of the infrastructure include nodes in a cellular network or intelligent traffic signs that can be utilized to establish car-industry communication, infotainment platforms or the Internet.
3. Car-to-X communication: This term refers to the sending and receiving of data between cars, the infrastructure, other transport, traffic management systems and different Internet applications. While other communications receive and process information, cars can also exchange information.
4. Smartphone or smart device: Given the implementation of common modern technology, smart phones, tablets and smart watch use is widespread and they become an obvious goal in the communication system, as shown in Figure-2.
5. Cloud: Computing can exchange data from cars and data stored in the (Cloud) by using the Internet, as shown in Figure-3.

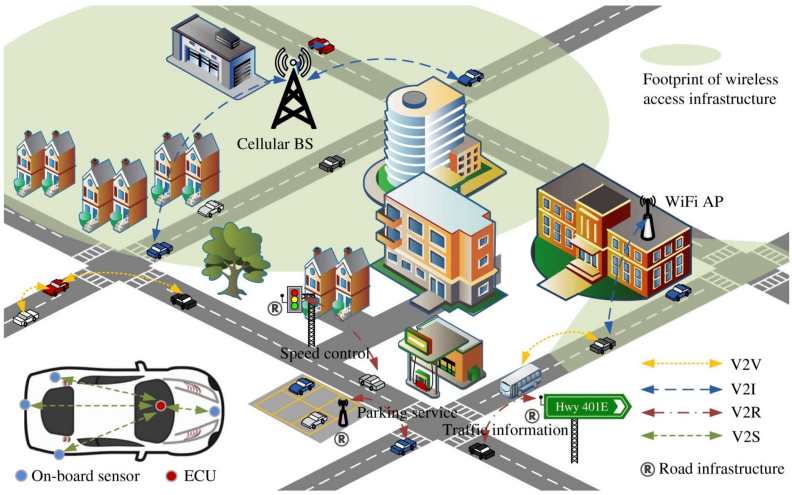

Fig. 2 Connection Types [32].

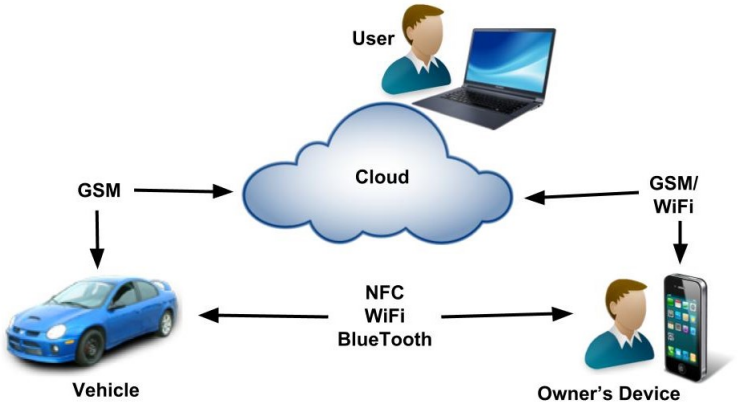

Fig. 3 Connection Types (Simple Car Connections

In recent years, electronic systems in vehicles have been controlled by an Electronic Control Unit (ECU). The controller Area Network (CAN) uses an in-vehicle network to structure an effective network of ECUs [57].

The ECU is an important component in automotive application components that can control one or more of the electrical systems and subsystems in cars [56]. The on-board architecture of vehicles can contain more than 70 ECUs [16] that can interconnect via different networks such as Local Interconnect Network (LIN), CAN or FlexRay [39, 1]. In fact, CAN use has become widespread because it significantly reduces the number of communication lines and ensures the reliability of higher data transmission [27], as shown in Figure-4. Recently, due to increasing penetration of smartphones and advanced communication technologies, Global Positioning System

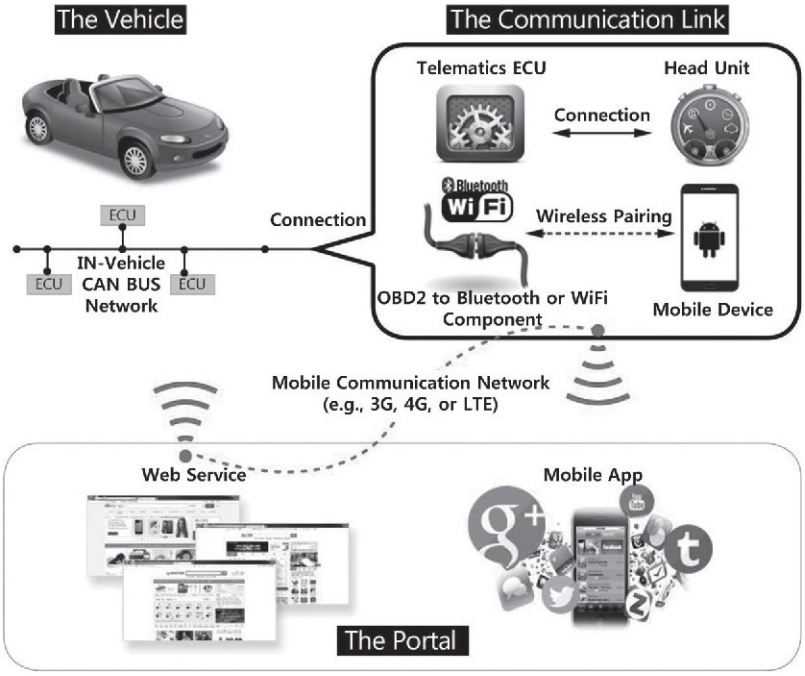

Fig. 4 Connection Types (Connected Car Environment [57]).

(GPS) data [53, 55], media access control (MAC) addresses from Bluetooth and Wi-Fi components [13, 19], and mobile phone data [14, 15] are becoming available for the analysis of traffic conditions or even travel behaviour and security in vehicles. The data sources listed above are important in developing and monitoring smart environments for intelligent cities. With such characteristics, more detailed analysis of attack, detect and defence of vehicle security could be conducted.

2.1 Attack

One of the effects of the extensive introduction of technology in vehicles is car hacking using malware [7]. Nowadays, it could be conducted to exploit a new generation of vehicles that are even more connected to wireless networks, to the Internet, and with each other [40], as shown in Figure-4. Vehicles in Vehicular Ad hoc Networks (VANETs) transmit self-information to fixed remote nodes such as their speed, direction, acceleration and traffic conditions. For example, Dedicated Short Range Communications (DSRC) are emerging as a standard to support IEEE 802.11 in communications between vehicles. FCC has allocated a 75 MHz of DSRC spectrum at 5.9 GHz to be used in VANETs communications. There is also an IEEE P1609 working group which has proposed DSRC as the IEEE 802.11p standard

which gives specifications for a wireless Medium Access Control (MAC) layer and a physical layer for Wireless Access in Vehicular Environments (WAVE) [38]. Attacks on VANETs create a large number of issues for all network users by using different types of attacks, such as malware [52]. In this chapter, two types of attacks using malware are addressed, namely, attacks on Inter-vehicle communication (IVC) and attacks on Intra-vehicle communication. Car methods are shown in Figure-1.

2.1.1 Attacks on Inter-vehicle communication (IVC)

Several years ago, work on Inter vehicle communication (IVC) started in industrial research labs and academic institutions. To date, some academic research teams have started addressing security issues in vehicles, however, some research projects are still highly theoretical and do not suggest realistic solutions [25]. In [44], various perspectives on IVC security were considered and the focus was on secure positioning and privacy problems. In this chapter, classifying and identifying the types of attacks in IVC aims to suggest practical solutions.

–Denial of Service Attack (DoS)
The purpose of (DoS) attacks is to prevent legal users from accessing services or data in computer networks. In vehicular networks, this attack jams and overflows the traffic with huge volumes of irrelevant messages that negatively affect communication among the nodes of the network, roadside units and on-board units. There is a huge number of high-powered computing facilities in close proximity to the target because the vehicle under attack is part of the vast infrastructure of the Social Internet of Vehicles (SIoV) embedded in a smart city environment. An attacker can use these for jamming attacks on the target's on-board sensory tool or use malware attacks, thereby countering the ability of the target vehicle to detect irregular messages during collaboration with its local information resources. A voting scheme can address the issues of DoS attacks [35]. However, if attackers can produce false identities to masquerade themselves, voting schemes may fail [31]. According to [33], DoS attacks have three levels:

First level (Basic Level): Overwhelm the Node Resources The goal of the attacker is to overwhelm the node resources so that other important and necessary tasks cannot be performed by their nodes. These nodes become constantly busy and use all the resources to check the messages.

• Case 01: DOS Attack in V2V Communications A warning message is sent by an attacker (Accident at location Y) and this message is received by a victim node behind the attacker node as shown in Figure-5. The attacker continuously repeats the sending of the same message, so the victim node is kept busy and is completely denied access to the network [45].

• Case 02: Launch DOS Attack in V2I Communications as shown in Figure-6, an attack is launched on a Road-Side Unit (RSU). Any other nodes that attempt to communicate with the RSU will be unable to get any response from the RSU, therefore, the service is unavailable when the RSU is continuously busy attempting

Fig. 5 DOS Attack in V2V Communications

to verify the messages. The key risk, in this example, is the inability to send critical life information [45].

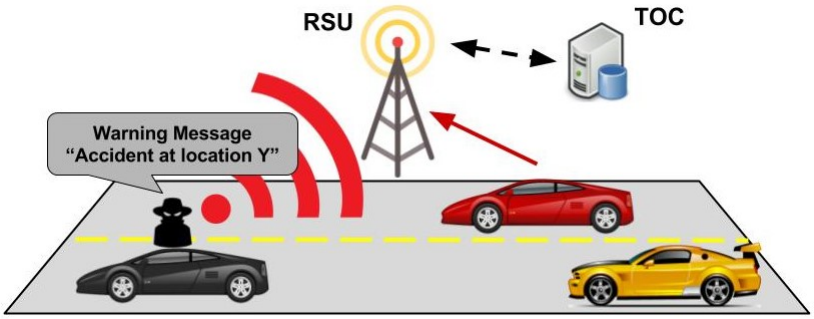

Fig. 6 Launch DOS Attack in V2I Communications

Second Level (Extended Level): Jamming the Channel The highest level of DOS attack involves Jamming the Channel, therefore, denying other users' access to the network. There are two possible cases:

• Case 01: A high frequency channel, sent by an attacker, jams the communication among any nodes in a domain as shown in Figure-7. Messages cannot be sent or received by these nodes in that domain (services are not available in that domain due to this attack). It can send and or receive messages when a node leaves the domain of attack [45].

• Case 02: Jamming the communication channel between the nodes and the infrastructure. In Figure-8, an attack is launched near the infrastructure to jam the channel. As a result, the network breaks down. In this way, because the network unavailable, sending and/or receiving messages and/or malware to/from other nodes is not possible and would fail.

Third Level: Distributed Denial of Services (DDOS): DDOS attacks are more serious in the vehicular ad hoc network (VANET) because of the distribution of this

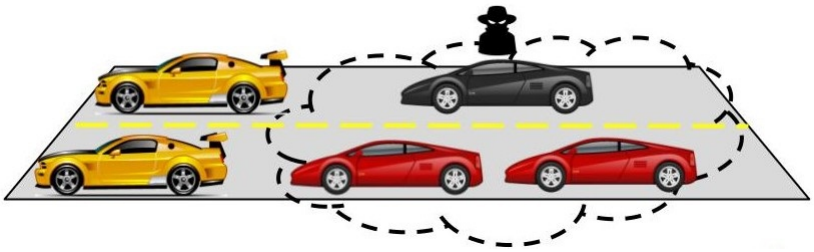

Fig. 7 A Domain of Jammed Channel for Vehicle-to-Vehicle Communications.

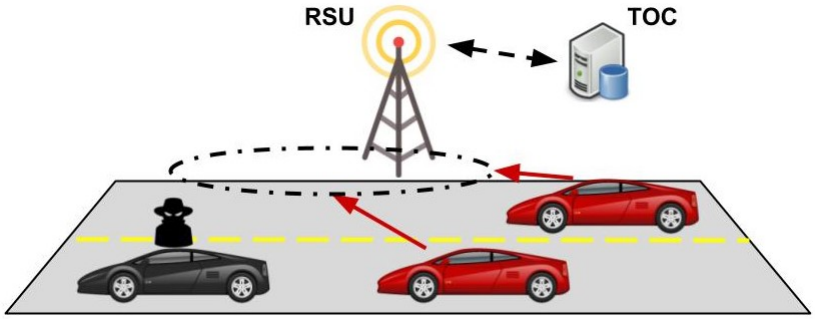

Fig. 8 Source: Denial of Service (DOS) Attack and Its Possible Solutions in VANET.

attack which spreads over a wide area of the network. The attacker can launch attacks from various resources. The two possible cases [26] are:

• Case 01: An attack is launched from various resources and different time slots may be used to send the messages. These messages and time slots may differ from node to node. The objective of this attack is to make a network unavailable by bringing the network down at a goal node. Figure-9 shows three attackers, black cars (nodes), sending messages to a red car (target node) in front. After a period of time, the goal node cannot connect with any other nodes in the network.

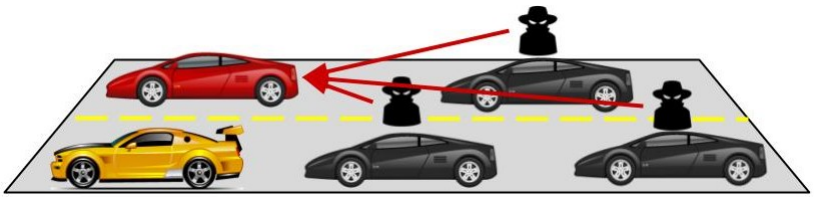

Fig. 9 DDOS in Vehicle-to-Vehicle Communications.

• Case 02: The VANET infrastructure (RSU) is the target of attack as shown in Figure-10. Three attackers in the network launch an attack on the infrastructure from

various sources. The infrastructure is overloaded, causing denial of service when other nodes in the network want to access the network.

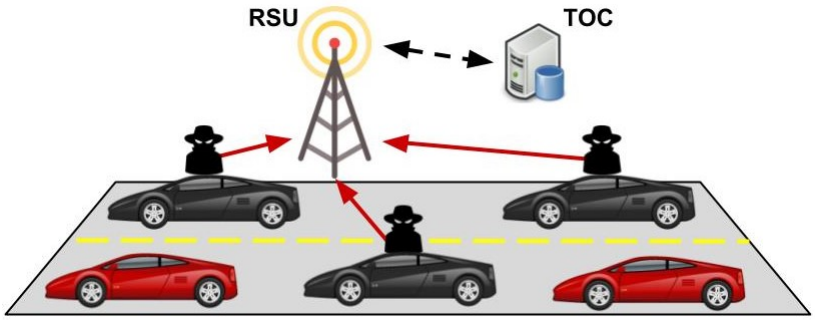

Fig. 10 DDOS in Vehicle-to-Infrastructure Communications.

– GPS Spooling Attack

This attack tries to fake a GPS Receiver by broadcasting false GPS signals, structured to match a set of normal GPS signals, or by rebroadcasting genuine signals captured elsewhere or at a different time. The attacker may modify these spoofed signals in such a way by using malware to cause the receiver to estimate its location to be somewhere other than where it actually is, or to be located where it is but at a different time. GPS spooling detection requires swiftness and accuracy. In many GPS based applications, it is critical to detect GPS spooling attacks as soon as possible, as shown in Figure-11. GPS has been used in wide area monitoring systems (WAMSs) in the power grid [62]. WAMS consist of frequency disturbance recorders (FDRs), a communication network and a monitoring system server. Each FDR is provided with a GPS receiver to obtain its position and accurate timing [49].

–Masquerading and Sybil

In a masquerading attack, a vehicle conceals its identity and appears to be legal in the vehicle network. Strangers can conduct attacks, such as injecting false messages or malware. In a Sybil attack, the attackers create several identities, appearing to be several legal vehicles at the same time. They can artificially damage a roadway and impact on the decision making of the other drivers during smart routing systems. In this attack mode, a vehicle can claim several locations concurrently, that can lead to traffic congestion [34].

– Impersonation Attack

The attackers steal the identity of a legal vehicle and can then broadcast security messages on the behaviour of that vehicle. These messages can affect the decision making of other drivers and generate traffic issues. In [18], a method called Building Up secure Connection along with Key factors (BUCK) has been proposed to detect and separate the impersonation attack.

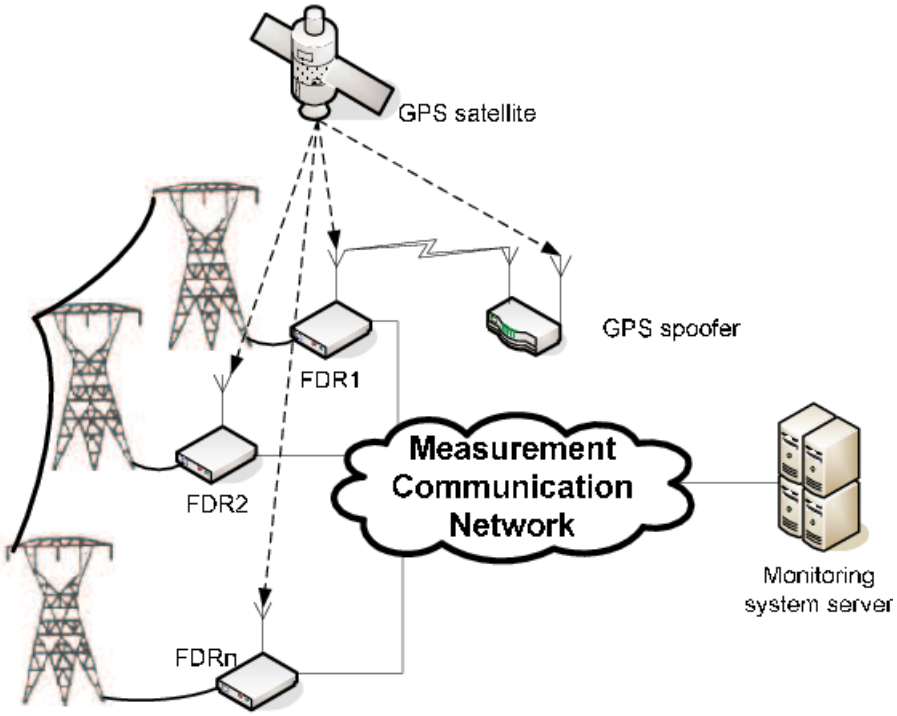

Fig. 11 Illustration of Time-Critical Spooling Detection in Power Grid System [32].

2.1.2 Attack on Intra Vehicle Communication

– Indirect physical access
In modern vehicles, the internal networks can be accessed either directly or indirectly by several physical interfaces:

- The OBD-II port, as shown Figure-12, is the most significant automotive interface that can provide direct access to the vehicle's key CAN buses. It provides service personnel with sufficient access to the full range of automotive systems, allowing routine maintenance for both diagnostics and ECU programming [17]. Attackers can also access the in-car entertainment system, for example, introducing false code into MP3files when playing the file and inserting malicious information and malware in the in-vehicle entertainment system without the owner's knowledge [60].
- Entertainment includes Disc, USB and iPod. A USB port or an iPod/iPhone docking port are external digital multimedia ports provided by vehicle manufacturers, allowing users to control their vehicle's media system by using their personal phone or audio player. Thus, an attacker can deliver malicious information and malware by using encoding algorithms as a song file on a CD and convincing the user to play it by using social engineering. Also, it may compromise an iPod or

the mobile phone of the user and install software on them that can help to attack the media system in a vehicle when connected.

Fig. 12 OBD-II [24].

– Short-Range Wireless Access

There are many drawbacks in indirect physical access to the network, including challenges to precise targeting, the inability to control the time of compromise and its operational complexity. Therefore, the ability of an attacker to locate a vehicle's wireless interface for devices is required to weaken that ability over a Short-Range Wireless Access [17]. Examples include the following:

- Bluetooth has been used to support hands-free calling in vehicles and it is sold by all vehicle manufacturers. Generally, Bluetooth devices used in vehicles have a range of 10 meters. The management services component of the Bluetooth stack is often implemented in software, while the Bluetooth protocol is typically implemented in hardware [44].
  For example, the attacker can place a wireless transmitter close to the vehicle's receiver device. The hackers need to know the vehicle's Bluetooth MAC address to exploit the vehicle's vulnerability without physical contact [60].
- Remote Keyless Entry: automobiles have been equipped with RF-based remote keyless entry (RKE) systems to open doors from a distance, flash lights, switch on the engine of the vehicle and activate alarms, as shown in Figure-13.
- Tire pressure: Modern vehicles have used a system to support a Tire Pressure Monitoring System (TPMS) to warn a driver about over or under inflated tires. It is called (Direct TPMS) and uses rotating sensors to transmit digital telemetry, as shown Figure 14.

Fig. 13 Remote Keyless Entry [36].

Fig. 14 Tire Pressure Monitoring System [3].

– Long-Range Wireless

Modern vehicles include long distance wireless digital access channels greater than 1 km. These comprise two categories (Adam, 2011):

- Broadcast channels are not specifically aimed at a given vehicle but can be (tuned into) by receivers on request to be a part of the external attack surface. Long-range broadcast media, such as control channels (to make attacks), can be attractive. Because they are difficult to detect, malware can control multiple receivers at once and does not need attackers to get an accurate address for their prey. There is a plethora of broadcast receivers for long-range signals in modern vehicles that include Global Positioning Systems (GPS) (Honda/Acura, GM, Toyota, Saab, Ford, Kia, BMW and Audi). Remote telematics systems are the most significant systems targeted in long range wireless attacks, with companies, such as Ford (Sync), GM (OnStar), and Toyota (Safety Connect) supplying their vehicles with data networks and cellular voices that provide numerous features, such as: (1) supporting safety (crash reporting); (2) convenience (hands free data access such as driving directions or weather); (3) diagnostics (early alert of mechanical issues); and (4) anti-theft (remote track and disable).

- Cellular channels also have many features vulnerable to attack over considerable distances by using malware, in a mostly covert way, because of the wide coverage of the cellular data structure and its relatively high bandwidth. Moreover, they are two-way channels ”supporting interactive control and data ex-filtration“ (Adam, 2011) and are individually addressable.

2.2 Defense

In the last decade, vehicle industries have been faced with critical security and privacy issues when they developed telematics systems. These issues relate to everyday applications that allow interfacing between vehicles and humans and vehicles and infrastructure. The current risks that face vehicle architectures are wireless security break-ins and sensors, but future automotive architectures and systems will increase these risks and, therefore, they need to be mitigated. Vehicle systems can be protected from (hackers) and infectious viruses using malware that will, from the consumer's perspective, have a direct impact on trustworthiness, the vehicle's safety dynamics and quality. Hacking occurs by taking full advantage of the telematics and wireless features that have become an important part of the vehicle, performing the function of an electrical system brain in the vehicle. Therefore, this allows the module to become the open input to the world. There are two potential solutions to defend against an attack [46]:

2.2.1 Inter-Vehicle Communication Solution

This solution combines cryptography and data security with the packet data session through (TCP/IP) and the voice service. A number of researchers have proposed trying to secure vehicle to vehicle Networks, but these methods are not sufficient to efficiently provide safety and security [46]. Many attempts have addressed this technique. In [21], a new technique was proposed, namely Elliptic Curve cryptography and Digital Signature Algorithms (ECDSA), by using two parties (a remote agent and network embedded system) to create a 128-bit symmetric key, and encrypting all transmitted data through the Advance Encryption Scheme (AES). An Identity-based Batch-Verification (IBV) technique that creates a private key for use in [61]. It does not require a certificate and it will verify each received signature within 300 ms. However, it relies on (the Dynamic Short-Range Communication (DSRC) protocols). The research of [43] investigated how much the Medium Access Control (MAC) protocol can acquire through both Quality of Service and security necessity for vehicle network safety applications and how to design an efficient MAC protocol to acquire the safety related vehicle networks.

2.2.2 Intra-Vehicle Communication Solution

As automotive industries began utilizing more and more electronics in vehicles, huge wire harnesses, that were expensive and heavy, were the result. Specific wiring was then replaced by in-vehicle networks, which reduced wiring weight, complexity, and cost. CAN, a high integrity serial bus system for intelligent networking devices, emerged as the standard in-vehicle network (see Figure-15). It requires data transmission security between the vehicle's ECU via a CAN Bus which is a protocol for an open and unsecured vehicle. Vehicle companies have no concerns about the security of this type of communication because of the low risk of remotely accessing the CAN Bus. The only way of accessing the CAN Bus is by using an On-Board Diagnostic (OBD) connector that can connect a diagnostic tool physically to the vehicle, so that problem analysis can be performed by authorized technicians [58]. However, automotive companies are able to easily develop hardware interfaces and software application layers that allow malware to access the CAN Bus directly through the telematics ECU by using Wi-Fi, BT and cellular networks. Today, technology has increased security risks to the point of allowing unauthorized systems and network access, audit ability and compliance, customer data breaches, internal and external sabotage, and the theft of intellectual property and confidential business information [50].

2.3 Detect

2.3.1 Challenges of Inter-Vehicle Communication

There is a critical problem in securing vehicle to vehicle or vehicle to infrastructure communication. This is because all communication between vehicle and vehicle or vehicle and roadside units occurs using wireless technology, therefore, if security is not enforced, the probability of various attacks or viruses being injected into

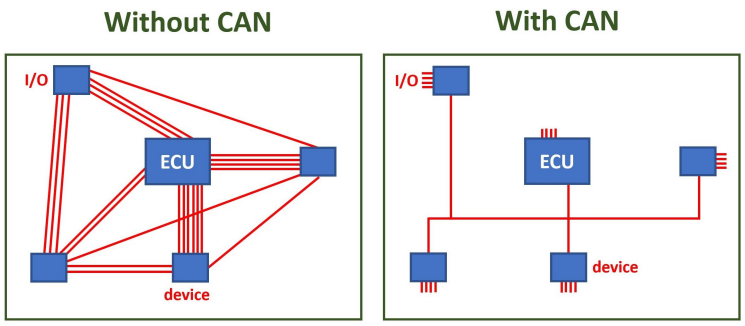

Fig. 15 A High-Integrity Serial Bus System with or without CAN.

the unprotected system is high [46]. Inter-Vehicle Communication still faces challenges regarding the following issues: trust; real-time communication; quality of service; message dissemination; fault detection; efficient physical layer transmission schemes; wireless network access; secure protocols; information security mechanisms; network scalability; and robustness [41]. Therefore, automotive industries need to create a secure, reliable and effective system to avoid these problems [46].

2.3.2 Challenges of Intra Vehicle Communication

Internal Vehicle Communication faces a range of issues [32]:

- The use of different generic wireless sensor networks possessing unique characteristics that provide the space for optimization.
- Sensors are stationary so that the network topology does not change over time.
- Sensors are typically connected to the ECU through one hop, which yields a simple star-topology.
- There is no energy constraint for sensors having a wired connection to the vehicle power system. The design and deployment of Internal Vehicle wireless sensor networks are still challenging.
- The Internal Vehicle Communication environment is difficult due to severe scattering in a very limited space and often with no line-of-sight. This is the major reason for the extensive effort to characterize the Internal Vehicle wireless channels.
- Data transmissions require low latency and high reliability to satisfy the stringent requirement of real-time Internal Vehicle control systems.
- Interference from neighbouring vehicles in a highly dense urban scenario may not be negligible.
- Security is critical to protect the in-vehicle network and control system from malicious attacks.

3 Recent Techniques and Challenges

Electrical wiring systems in vehicles have become increasingly sophisticated. They require more and more connectors, control units, relays and terminals to connect the ECU with other devices. Recently, due to developments in automotive technology, vehicles have become even more connected through wireless networks and have become more dependent on complex electronic systems. Therefore, vehicles can be attacked through wireless networks, smartphones, GPS and cameras [59]. Automotive industries, such as AVnu and OPENSIG, argue that Ethernet represents the standard of next-generation automotive networks because ethernet is wide-ranging and includes band width improvements, improved implementation, flexibility and cost savings. Currently, it is not convenient to replace all in-vehicle devices with Ethernet enabled replacements [42]. Thus, it is likely that Ethernet will function as a

high-speed backbone network at first, coexisting with legacy technologies until such time it becomes cost effective to migrate to a full end-to-end Ethernet solution. As automotive networks become more complicated, the standardization of approaches becomes more and more attractive to manufacturers. This is happening at all levels of the automotive communication stack and is gaining momentum, with organizations such as IEEE RTPGE, OPENSIG, the AVnu alliance, and AUTOSAR coordinating an industry-led push toward extensible and cost effective standards that will drive the development of in-vehicle networks, as shown in Figure-16. Research in this field has been increased. For example, in [26], a method of V2I cybersecurity architecture, known CVGuard, can detect and prevent cyber-attacks on V2I applications. A Stop Sign Gap Assist (SSGA) application has shown that CVGuard was effective in mitigating the adverse safety effects created by a DDoS attack.

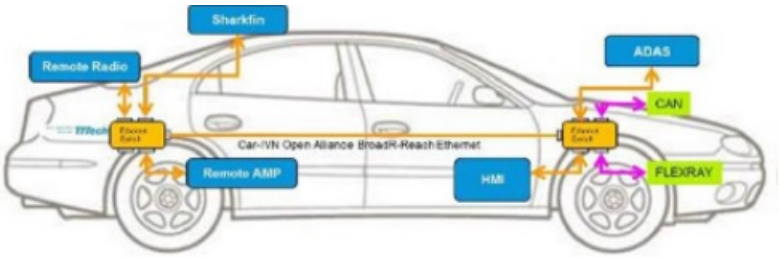

Fig. 16 Ethernet Switch to Connect Vehicle's Devices [28, 30].

The literature suggests that, as in-vehicle technology becomes more and more complex, there will be a drive to standardize approaches across the industry, allowing manufacturers to focus on improving the existing applications built on similar foundations. This provides an excellent structure for the future expansion and improvement of in vehicle network systems and leads, ultimately, to greater driver comfort and, most importantly, safety [54].

4 Conclusion

Developing security solutions compatible with the automotive ecosystem and smart cities is challenging and we believe it will require greater engagement between the computer security community and automotive manufacturers. This chapter provides an opportunity to reflect on the security and privacy risks and malware associated with modern automobiles. We synthesized concrete, pragmatic recommendations for future automotive security and identified fundamental challenges. Defending against known vulnerabilities does not mean the non-existence of other vulnerabilities, thus, many of the specific vulnerabilities identified will need to be addressed. In the future,

it may be that the future of intelligent transportation systems and smart cities falls within the multiple layers of the connected environment including Cyber-security and forensics [5], artificial intelligence and machine learning in identification traffic [10], biometric recognition [2, 8, 4], traffic congestion control based In-Memory Analytics [6] and connected networks of vehicles. These will lead to the development of future intelligent transportation systems and smart cities and vehicle industries that include the analysis of information regarding malware from cyber sources, CSP network modelling, and flow models in a connected environment.

References

[1] Saber A., Di Troia F., and Stamp M. Intrusion detection and can vehicle networks. *Digital Forensic Investigation of Internet of Things (IoT) Devices*, 2020.

[2] Khamael Abbas. Eye recognition technique based on eigeneyes method. In *International Conference on Software and Computer Applications*, volume 9, pages 212–219. IACSIT Press, Singapore, 2011.

[3] Adam. Tire pressure, 2011. Retrieved from: http://www.bergenimports.com/tire-pressure.

[4] Khamael Abbas Al-Dulaimi and Aiman Abdul Razzak Al-Saba'awi. Handprint recognition technique based on image segmentation for recognize. *International Journal of Computer Information Systems*, 2(6):7–12, 2011.

[5] Aiman Al-Sabaawi and Ernest Foo. A comparison study of android mobile forensics for retrieving files system. *International Journal of Computer Science and Security (IJCSS)*, 13(4):148, 2019.

[6] Aiman Abdul-Razzak Fatehi Al-Sabaawi. Traffic congestion control based in-memory analytics: Challenges and advantages. *International Journal of Computer Applications*, 975:8887, 2017.

[7] M. Alazab, S. Venkatraman, and P. Watters. *Information Security Governance: The Art of Detecting Hidden Malware*. IGI Global, 2013.

[8] S. M. Ali and Khamael A. AL-Phalahi. Face recognition technique based on eigenfaces method. In *3rd Scientific Conference of the College of Science-Baghdad University-Iraq*, pages 781–785, 2009.

[9] C Atombo, C Wu, H Zhang, and AA Agbo. Drivers speed selection behaviors, intention, and perception towards the use of advanced vehicle safety. *Advances in transportation studies*, 42:23–38, 2017.

[10] A. Azab, M. Alazab, and M. Aiash. Machine learning based botnet identification traffic. In *2016 IEEE Trustcom/BigDataSE/ISPA*, pages 1788–1794, 2016.

[11] A. Azab, R. Layton, M. Alazab, and J. Oliver. Mining malware to detect variants. In *2014 Fifth Cybercrime and Trustworthy Computing Conference*, pages 44–53, 2014.

[12] Tamás Bécsi, Szilárd Aradi, and Péter Gáspár. Security issues and vulnerabilities in connected car systems. In *2015 International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS)*, pages 477–482. IEEE, 2015.

[13] Ashish Bhaskar and Edward Chung. Fundamental understanding on the use of bluetooth scanner as a complementary transport data. *Transportation Research Part C: Emerging Technologies*, 37:42–72, 2013.

[14] N Caceres, JP Wideberg, and FG Benitez. Deriving origin–destination data from a mobile phone network. *IET Intelligent Transport Systems*, 1(1):15–26, 2007.

[15] Francesco Calabrese, Mi Diao, Giusy Di Lorenzo, Joseph Ferreira Jr, and Carlo Ratti. Understanding individual mobility patterns from urban sensing data: A mobile phone trace example. *Transportation research part C: emerging technologies*, 26:301–313, 2013.

[16] Robert N Charette. This car runs on code. *IEEE spectrum*, 46(3):3, 2009.

[17] Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, Tadayoshi Kohno, et al. Comprehensive experimental analyses of automotive attack surfaces. In *USENIX Security Symposium*, volume 4, pages 447–462. San Francisco, 2011.

[18] Simranpreet Singh Chhatwal and Manmohan Sharma. Detection of impersonation attack in vanets using buck filter and vanet content fragile watermarking (vcfw). In *2015 International Conference on Computer Communication and Informatics (ICCCI)*, pages 1–5. IEEE, 2015.

[19] Antonin Danalet, Bilal Farooq, and Michel Bierlaire. A bayesian approach to detect pedestrian destination-sequences from wifi signatures. *Transportation Research Part C: Emerging Technologies*, 44:146–170, 2014.

[20] G Dedes, S Wolfe, D Guenther, Byungkyu Brian Park, JJ So, K Mouskos, D Grejner-Brzezinska, C Toth, X Wang, and G Heydinger. A simulation design of an integrated gnss/inu, vehicle dynamics, and microscopic traffic flow simulator for automotive safety. *Advances in Transportation Studies*, 2011.

[21] Roshan Duraisamy, Zoran Salcic, Maurizio Adriano Strangio, and Miguel Morales-Sandoval. Supporting symmetric 128-bit aes in networked embedded systems: An elliptic curve key establishment protocol-on-chip. *EURASIP Journal on Embedded Systems*, 2007:1–9, 2007.

[22] Konstantinos Fysarakis, Ioannis Askoxylakis, Vasilios Katos, Sotiris Ioannidis, and Louis Marinos. Security concerns in co-operative intelligent transportation systems. 2017.

[23] Andy Greenberg. Hackers remotely kill a jeep on the highway—with me in it. *Wired*, 7:21, 2015.

[24] Harborfreigh. OBD II and can code reader with multilingual menu, 2016. Retrieved from:http://www.harborfreight.com/ can-obdii-code-reader-with-multilingual-menu 98568.html.

[25] Jean-Pierre Hubaux, Srdjan Capkun, and Jun Luo. The security and privacy of smart vehicles. *IEEE Security & Privacy*, 2(3):49–55, 2004.

[26] Mhafuzul Islam, Mashrur Chowdhury, Hongda Li, and Hongxin Hu. Cybersecurity attacks in vehicle-to-infrastructure applications and their prevention. *Transportation research record*, 2672(19):66–78, 2018.

[27] Karl Henrik Johansson, Martin Törngren, and Lars Nielsen. Vehicle applications of controller area network. In *Handbook of networked and embedded control systems*, pages 741–765. Springer, 2005.

[28] S. Koopman. Automotive advanced driver assistance systems ADAS market will reach $ 18.2bn in 2014. According to a New Study on ASDReports, 2015. https://www.asdreports.com/news-5198/automotive-advanced-driver-assistance-systems-adas-market-will-reach-182bn-2014-according-new-study-asdreports.

[29] Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak Patel, Tadayoshi Kohno, Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, et al. Experimental security analysis of a modern automobile. In *2010 IEEE Symposium on Security and Privacy*, pages 447–462. IEEE, 2010.

[30] Reger L. Advances in automotive at ces 2015, 2015. Retrieved from: https://blog.nxp.com/automotive/advances-in-automotive-at-ces-2015.

[31] Victor Lesser, Charles L Ortiz Jr, and Milind Tambe. *Distributed sensor networks: A multiagent perspective*, volume 9. Springer Science & Business Media, 2012.

[32] Ning Lu, Nan Cheng, Ning Zhang, Xuemin Shen, and Jon W Mark. Connected vehicles: Solutions and challenges. *IEEE internet of things journal*, 1(4):289–299, 2014.

[33] Leandros A Maglaras, Ali H Al-Bayatti, Ying He, Isabel Wagner, and Helge Janicke. Social internet of vehicles for smart cities. *Journal of Sensor and Actuator Networks*, 5(1):3, 2016.

[34] Leandros A Maglaras, Pavlos Basaras, and Dimitrios Katsaros. Exploiting vehicular communications for reducing co2 emissions in urban environments. In *2013 International Conference on Connected Vehicles and Expo (ICCVE)*, pages 32–37. IEEE, 2013.

[35] Adil Mudasir Malla and Ravi Kant Sahu. Security attacks with an effective solution for dos attacks in vanet. *International Journal of Computer Applications*, 66(22), 2013.

[36] Maurizio. Hacking car security system and remote keyless entry, 2015. Retrieved from: http://dev.emcelettronica.com/hacking-car-security-system-and-remote-keyentry-rke.

[37] Hamid Menouar, Ismail Guvenc, Kemal Akkaya, A Selcuk Uluagac, Abdullah Kadri, and Adem Tuncer. Uav-enabled intelligent transportation systems for the smart city: Applications and challenges. *IEEE Communications Magazine*, 55(3):22–28, 2017.

[38] Bassem Mokhtar and Mohamed Azab. Survey on security issues in vehicular ad hoc networks. *Alexandria engineering journal*, 54(4):1115–1126, 2015.

[39] Thomas Nolte, Hans Hansson, and Lucia Lo Bello. Automotive communications-past, current and future. In *2005 IEEE Conference on Emerging Technologies and Factory Automation*, volume 1, pages 8–pp. IEEE, 2005.

[40] Paganini P. Car hacking is today possible due the massive introduction of technology in our vehicles, 2013. Retrieved from: https://www.cyberdefensemagazine.com/car-hacking-is-today-possible-due-the-massive-introduction-of-technology-in-our-vehicles.

[41] Vineetha Paruchuri. Inter-vehicular communications: Security and reliability issues. In *ICTC 2011*, pages 737–741. IEEE, 2011.

[42] Donovan Porter. 100base-t1 ethernet: the evolution of automotive networking. *Texas Instruments, Techn. Ber*, 2018.

[43] Yi Qian, Kejie Lu, and Nader Moayeri. Performance evaluation of a secure mac protocol for vehicular networks. In *MILCOM 2008-2008 IEEE Military Communications Conference*, pages 1–6. IEEE, 2008.

[44] Maxim Raya and Jean-Pierre Hubaux. Security aspects of inter-vehicle communications. In *5th Swiss Transport Research Conference (STRC)*, number CONF, 2005.

[45] Syed Rizvi, Jonathan Willet, Donte Perino, Seth Marasco, and Chandler Condo. A threat to vehicular cyber security and the urgency for correction. *Procedia computer science*, 114:100–105, 2017.

[46] Mustafa Saed, Scott Bone, and John Robb. Security concepts and issues in intra-inter vehicle communication network. In *Proceedings of the International Conference on Security and Management (SAM)*, page 1. The Steering Committee of The World Congress in Computer Science, Computer . . . , 2014.

[47] Florian Sagstetter, Martin Lukasiewycz, Sebastian Steinhorst, Marko Wolf, Alexandre Bouard, William R Harris, Somesh Jha, Thomas Peyrin, Axel Poschmann, and Samarjit Chakraborty. Security challenges in automotive hardware/software architecture design. In *2013 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pages 458–463. IEEE, 2013.

[48] G. Samuel. Jeep owners urged to update their cars after hackers take remote control, 2015. https://www.theguardian.com/technology/2015/jul/21/jeep-owners-urged-update-car-software-hackers-remote-control.

[49] Nils Sparwasser, Markus Stöbe, Hartmut Friedl, Thomas Krauß, and Robert Meisner. Simworld–automatic generation of realistic landscape models for real time simulation environments–a remote sensing and gis-data based processing chain. *Advances in transportation studies*, 21, 2007.

[50] W. Stallings. Cryptography and network security: principles and practice. Upper Saddle River: Pearson, 2017.

[51] Agachai Sumalee and Hung Wai Ho. Smarter and more connected: Future intelligent transportation system. *IATSS Research*, 42(2):67–71, 2018.

[52] Irshad Ahmed Sumra, Halabi Bin Hasbullah, Iftikhar Ahmad, Daniyal M Alghazzawi, et al. Classification of attacks in vehicular ad hoc network (vanet). *International Information Institute (Tokyo). Information*, 16(5):2995, 2013.

[53] Dihua Sun, Hong Luo, Liping Fu, Weining Liu, Xiaoyong Liao, and Min Zhao. Predicting bus arrival time on the basis of global positioning system data. *Transportation Research Record*, 2034(1):62–72, 2007.

[54] Shane Tuohy, Martin Glavin, Ciarán Hughes, Edward Jones, Mohan Trivedi, and Liam Kilmartin. Intra-vehicle networks: A review. *IEEE Transactions on Intelligent Transportation Systems*, 16(2):534–545, 2014.

[55] Lelitha Vanajakshi, Shankar C Subramanian, and R Sivanandan. Travel time prediction under heterogeneous traffic conditions using global positioning system data from buses. *IET intelligent transport systems*, 3(1):1–9, 2009.

[56] Marko Wolf, André Weimerskirch, and Thomas Wollinger. State of the art: Embedding security in vehicles. *EURASIP Journal on Embedded Systems*, 2007:1–16, 2007.

[57] Samuel Woo, Hyo Jin Jo, and Dong Hoon Lee. A practical wireless attack on the connected car and security protocol for in-vehicle can. *IEEE Transactions on intelligent transportation systems*, 16(2):993–1006, 2014.

[58] Aastha Yadav, Gaurav Bose, Radhika Bhange, Karan Kapoor, NCSN Iyengar, and Ronnie D Caytiles. Security, vulnerability and protection of vehicular on-board diagnostics. *International Journal of Security and Its Applications*, 10(4):405–422, 2016.

[59] Teng Yang, Frank Wolff, and Chris Papachristou. Connected car networking. In *NAECON 2018-IEEE National Aerospace and Electronics Conference*, pages 60–64. IEEE, 2018.

[60] J. Yoshida. How hackers can take control over your car. EE Times, 2013. https://www.eetimes.com/document.asp?doc_id=1318838&page_number=2.

[61] Chenxi Zhang, Rongxing Lu, Xiaodong Lin, P-H Ho, and Xuemin Shen. An efficient identity-based batch verification scheme for vehicular sensor networks. In *IEEE INFOCOM 2008-The 27th Conference on Computer Communications*, pages 246–250. IEEE, 2008.

[62] Yingchen Zhang, Penn Markham, Tao Xia, Lang Chen, Yanzhu Ye, Zhongyu Wu, Zhiyong Yuan, Lei Wang, Jason Bank, Jon Burgett, et al. Wide-area frequency monitoring network (fnet) architecture and applications. *IEEE Transactions on smart grid*, 1(2):159–167, 2010.