Investigating Security Vulnerabilities in Modern Vehicle Systems

Xi Zheng[1(✉)], Lei Pan[1], Hongxu Chen[2], and Peiyin Wang[1]

[1] Deakin University, Geelong, VIC 3220, Australia
{xi.zheng,l.pan,peiyinw}@deakin.edu.au
[2] State Key Laboratory of Automotive Safety and Energy, Tsinghua University, Beijing, China
herschel.chen@gmail.com

Abstract. Modern vehicle systems have evolved from an isolated control system into an interconnected architecture combining software, hardware, and data. Such architecture is specialized into vehicle infotainment system (e.g., SYNC of Ford, iDrive of BMW and MMI of Audi), Vehicle to Vehicle (V2V), Vehicle to Infrastructure (V2I), and vehicle social system which connects to social media networks. These systems hold private and sensitive information such as travel plans, social network messages, login credentials to bank accounts, and so on, which is a lucrative target for malicious attackers. Unfortunately, existing research overlooks the security issues with respect to this highly integrated system. This paper presents security issues across various systems related to modern vehicles through a a holistic and systematic view. We analyze each system components with respect to published attacks in details and present a synthesized body of knowledge. We identify the growing trend where security attacks are launched from the cyber space to vehicle control system via smartphones and vehicle networks. In the foreseeable future, we expect more security attacks both in numbers and in complexity. Knowing this will arise the awareness of vehicle system security and help engineers to build security solutions.

Keywords: Evaluation of security · Authentication and authorization · Distributed systems security · Privacy protection · Smartphone security · Modern vehicle system · Security · Privacy · Reliability

1 Introduction

Nowadays, automobile manufacturers integrate car control system (e.g., CAN bus) with mobile applications, which in turn evolves into a multi-function vehicle system named vehicle infotainment system. Vehicle infotainment system differs from traditional vehicle system which typically has audio playing function with several buttons. Vehicle infotainment system provides more interaction between drivers/passengers and vehicle systems, which allows drivers to monitor their cars and to achieve advanced functions such as making hand-free calls, sending

L. Batten and G. Li (Eds.): ATIS 2016, CCIS 651, pp. 29–40, 2016.
DOI: 10.1007/978-981-10-2741-3_3

voice messages, establishing Bluetooth connection and so on. To utilize the information outside a vehicle, Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) system enables the communications and interaction among nearby vehicles or road infrastructures. The V2V system aims to share the information related to traffic information and accident warning among nearby vehicles or road infrastructures, to improve the road and drivers' safety. Based on V2V and V2I, the concept of social networking was brought into the area of the vehicle system. Drivers can share their experiences and useful information to other drivers via the Internet not only restricted to nearby vehicles. Hence, Vehicle to Social (V2S) system is the future trend of current modern vehicle systems.

The introduction of these new systems inside vehicles increases the level of security risks. For example, some latest vehicles can be hacked within 360 s [38]; actuators of the modern vehicles can be remotely controlled; terrorists can potentially hack into V2V and V2I to cause chaotic traffic accidents (e.g., to hack into an autonomous intersection system [7]), stealing privacy information from any driver. Many research work have been done for modern vehicle systems to cover the design, control, and automation of vehicles [8,12,20,30,39], or to cover vulnerability issues in a specific system (e.g., control system [31], vehicle to vehicle communication [37], vehicle networks [14], in-car wireless network [17]).

However, there is a significant gap in the current research. On one hand, researchers are not fully aware of the security impact of introducing the new features. Thus, no comprehensive analysis is yet provided to cover these features. On the other hand, car manufacturers are not aware of what security vulnerabilities possible in those features they have introduced or going to introduce to the modern vehicle systems which researchers have potential to help. Therefore, this paper first analyses these modern vehicle systems, and then discusses the vulnerabilities in these systems and proposes potential solutions. Overall, this paper makes the following two research contributions:

- We analyze features of modern vehicle systems.
- We analyze open problems and challenges for these modern vehicle systems in terms of security and reliability.

The rest of paper is organized as follows. Section 2 introduces the features of modern vehicle systems. The security challenges associated with these features are presented in Sect. 3. In Sect. 4, we summarize some related works. And we conclude this paper in Sect. 5.

2 Background

2.1 Vehicle Network Control System

The vehicle network control system connects all components of vehicle, where Controller Area Network (CAN) [9] is widely used in most vehicles. According to [9], CAN provides two layers of the Open Systems Interconnection (OSI): the physical layer and the data link layer. CAN protocol gains its popularity because

of its open design and good performance in data transmission. However, CAN also has obvious limitations: big and variable pulse, lack of clock synchronization, finite speed-distance ratio, inflexible design, data conformance problem, finite error control, and limited support for fault tolerance [9].

2.2 Vehicle Infotainment System

Vehicle infotainment system provides user-friendly functions, such as hand-free call, checking SMS, controlling audio player, mobile device support, and other accessories which can improve drivers' experience. A comprehensive vehicle infotainment system provides some safety and security functions, such as to monitor vehicle status (i.e. tire pressure, and road condition using 360-degree camera). Meanwhile, vehicle infotainment system also serves passengers, a rear seat infotainment system is usually provided on some luxury vehicles, such as Mercedes-Benz S-series, BMW 7 series, and Audi A8 series etc. The rear seat infotainment system has the same function with drivers' one. It controls audio/video player, checks vehicle running status, controls navigation, and browses web contents [28].

In the current vehicle market, almost each automobile manufacturer has its own vehicle infotainment system, such as SYNC of Ford, iDrive of BMW, and MMI of Audi. In recent years, some players in the software industry also try to access the area of vehicle infotainment system and become an emerging member, such as NVIDIA and Apple.

Moreover, drivers now prefer to tap their smartphone to control this system [11]. Tesla [36] launched Model S in 2012, which is the first premium electric sedan. And there is a 17-inch display touch screen installed into Model S, which offers the largest display touch screen among selling vehicles. This touch screen is powered by NVIDIA's Tegra [35], it has climate control, navigation, and display vehicle information. The driver can download the "Tesla Motors"application via Google Play and App Store, which can monitor and control their car with their mobile device remotely. When the user finishes download and installation, they can use their'My Tesla' account to log in and access this application. This application provides several functions: keyless driving, range status, climate control, and GPS location. After successfully installing and connect with their Tesla Model S, the vehicle owner can unlock and drive their car without the key, they also can check current range and charge status. In addition, the car owner can use this application to turn on the climate control system and vent sunroof remotely. The vehicle's parked location will be provided when car owner forget where did they park.

SYNC is used on Ford, Lincoln, Mercury, and Flex models, which is developed based on Microsoft Auto platform. SYNC can also handle most media players in the current market: iPod (Apple), Zune (Microsoft), and MP3 files which are stored in the USB or SD card [34]. The latest version (version 3) of SYNC also has the system update service over Wi-Fi, enhanced voice recognition, high-speed performance, and Apples Siri [3] seamless integration.

Apple launched its in-vehicle infotainment system called CarPlay [2], which is based on Blackberry's QNX platform. This system allows iPhone user to

use maps, send messages, listen to music, and make calls. Apple listed several committed partnerships, including Mercedes-Benz, Ferrari, Volvo, PORSCHE, GMC, and Volkswagen. In addition, CarPlay is compatible with all iPhone models after iPhone 5.

2.3 Vehicle to Vehicle (V2V) and Vehicle to Infrastructure System (V2I)

The setup of Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) enables communications between vehicles and infrastructure so that useful road information and emergency messages can be exchanged. These systems aim to reduce the rate of accidents, and increase the safety of the road users. To achieve efficient communications among vehicles and infrastructures, Vehicular Ad Hoc Networks (VANETs) is introduced as the base for V2V and V2I systems [13].

However, VANETs are facing some technical challenges and socio-economic challenges, among which bandwidth and dynamic network topology received a lot of attention. For instance, when the communication starts, can the underlying network hold huge information during traffic peak hours? Meanwhile, how modern vehicle system interact with infrastructure while vehicle itself is moving at a fast speed? What useful information can be shared by infrastructure to the vehicle system to maintain an optimum level of performance?

In [33], an architecture of Vehicular Communications (VC) is presented, which includes inter-vehicle communications (IVC), hybrid-vehicle communications (HVC), and roadside-vehicle communications (RVC). Meanwhile, inter-vehicle communications (IVC) is divided into two types of system: the single-hop system and the multi-hop system.

Nowadays, Vehicle to Vehicle communication system is usually used to provide some warning messages or notifications, such as Cooperation Collision Warning to avoid accident. In [41], it shows that the emerging wireless technologies were used for Dedicated Short Range Communications (DSRC) [6]. In [6], it is shown that 60 % of collision can be avoided by using some warning mechanisms. As the analysis of collision warning, a V2V application should be developed to support the system operation.

There are two approaches for developing the V2V applications — passive or active.

- The passive approach needs all the vehicles nearby to communicate using the same application. Then important information can be updated and exchanged at real time among the vehicles nearby. When the traffic congestion happened, the network however might suffer from communication saturation due to huge amount of data communicated.
- In comparison, the active approach will select the vehicle, which might face emergency situation, to send an Emergency Warning Messages (EWMs). The active approach can avoid network saturation in peak hour.

In order to decrease congestion time and air pollution level, V2I system can be seen as a possible solution to this environmental issue. In [21], V2I system can

provide some audio messages of traffic to the vehicle system, which can help to improve driving performance with a smooth speed. Meanwhile, V2I system can also be used to notify emergency situations to drivers. For example, sometimes drivers cannot react to the change of traffic lights during the daytime when they approach intersections due to sun glare. Now drivers can receive an audio message from roadside infrastructure to notify the change of traffic light. Another application of V2I in people daily trip is that it can notify ahead road work. When drivers drive with a high speed, they cannot realize the speed limit and reduce their speed to the speed limit required for the ahead road work. Therefore, V2I system can be used to send audio messages to drivers and notify the information of ahead road work zone. A roadside infrastructure system will help the driver to avoid accidents happened. Meanwhile, In [21], it points out V2I system can also reduce vehicle emissions due to improved driving efficiency. When V2I system is used, most of car emissions, including nitrogen dioxide, hydrocarbons, carbon monoxide, carbon dioxide, have been reduced with smallest reduction in carbon dioxide emission (around 7 %) and biggest reduction in carbon monoxide (around 32 %).

In [13], it shows that there are safety-related applications of Vehicle Safety Communication (VSC): signal violation warning, curve speed warning, emergency electronic brake light, pre-crash sensing, cooperative forward collision warning, left turn assistant, lane-change warning and stop sign movement assistant.

2.4 Vehicle Social System

The automobile manufacturers and software providers are not confined to V2V and V2I systems, they have started to shift the focus towards the communications between vehicles and social medias.

With network widely used in people's daily life, people can obtain more information from the internet. People also can share their experience and information anytime and anywhere. For the vehicle social system, drivers can share their experiences and useful information to other drivers via the internet. It is not only restricted to communicate and interaction among nearby vehicles. Therefore, Vehicle to Social (V2S) system is going to play a major role in the future vehicle systems. The following graph is a prototype of Vehicle Social Networks (VSNs). There are some communications and interactions between vehicles and signal towers, mobile devices and signal tower, and people and signal tower.

In [23], with the development of online social networks, a new type of ad hoc networks was introduced called Vehicular Social Networks (VSNs). VSNs can be used to implement Intelligent Transportation System (ITS). VSNs aims to improve the road and drivers' safety, as well as to reduce the traffic congestion. In [23], a new system prototype was implemented, which called SocialDrive and the concept and architecture of SocialDrive were also provided in the case study. In [32], an advanced social network prototype was presented, where real-time road conditions are shared via cloud.

SocialDrive is a novel prototype of vehicle social system, it provide data sharing and data receiving function. SocialDrive aims to publish the dynamic data and information to other vehicles, meanwhile, receive messages from other vehicles. In their study, an example of SocialDrive is provided: There are five hypothetical vehicles on the road. If the first and last vehicle want to share data, but the distance is not enough so that the data can only be received by the third vehicle. SocialDrive can gather these data and make the third vehicle as a center to share different data to other vehicles.

3 Analysis of Possible Security Attacks

3.1 Vehicle Network Control System Attacks

Many protocols are adopted to implement the vehicle network. According to [19], all vehicles sold in the United State are required to implement the Controller Area Network (CAN) bus (ISO 11898) for diagnostics. Meanwhile, CAN is facing security challenges due to broadcast nature, vulnerability to denial of service attack, no authenticator fields, weak access control, and Electronic Control Units (ECUs) firmware updates and open diagnostic control [19].

In [5], many essential components of modern vehicles, including gearbox, climate control, ignition system, and electrical window control, are now controlled by ECUs as embedded systems. ECU is one of the most important parts of a vehicle, and there are about 90 ECUs in the luxury-class vehicles [5]. Due to the huge number of ECUs installed on the vehicle, ECUs are also facing security issues: modifying code, reverse engineering, fuzzing attack, and phlashing attack. For instance, the attacker can modify the programming code during design and implementation processing. The data is the target for the attackers to achieve the purpose of corruption or degradation of hardware performance, and destroy of information.

In [15], the electronic window lift system can be attacked by the attacker via CAN bus. The attackers can use real hardware to attack the electronic window lift system, thus, to attack the anti-theft system and airbag system's warning lights on the dashboard.

In [25], a vehicle virus was created which can capture the messages delivered by CAN bus. Upon successful capture of door locking messages, this virus can lock the vehicle's doors remotely. As a connection media to all vehicle components, security issues in CAN bus bring huge risks to drivers' safety and privacy. Hackers can hack the networked control system and control vehicle easily. The hackers can configure the setting, modify the code, implant virus and malware. Therefore, it is of vital importance to address these security issues during the development and implementation process.

3.2 Vehicle to Vehicle and Vehicle to Infrastructure System Attacks

As previously mentioned in Sect. 2, VANETs is used to enhance drivers' safety (i.e., collision warning, Blind Spot Information System (BLIS)) and comfort

(i.e., locating gas station, tollway and parking payment, and internet access). Intelligent Transportation Systems is used to reduce traffic congestion, and both road and vehicle safety are also improved.

The main vulnerabilities of dense VANETs are caused by the lack of fixed infrastructure to protect the security and privacy in the application of wireless networks and application of Medium Access Control (MAC) 802.11 layer [5,16,18]. It directly implies eavesdropping attacks.

In current society, Vehicle to Vehicle (V2V) system can be used to send messages among the vehicles. V2V system should be designed with high reliability and low delay when the messages are sent. Because drivers need the sufficient amount of time to react to the emergency situations. In order to ensure the high reliability and low delay, simple mechanisms without high level security protection are used in the V2V system such as Medium Access Control (MAC) and 802.11a radio. In [40], the reliability of receiving messages in VANETs can be greatly affected due to issues in transmission collision and transmission power in the wireless ad hoc network.

In general, VANETs threats can be summarized into three aspects: confidentiality, authenticity, and availability.

- Threats of confidentiality mainly refer to that the communications among vehicles have been eavesdropped, which lead to important information of vehicles illegally collected without permission. For instance through eavesdropping processing, attackers can collect the privacy information to know the location of driver.
- For threats to authenticity, there are several types of attack for Vehicular Ad Hoc Network (VANET): Sybil attack, bogus information, man in the middle attack (MiMA), Global Positioning System (GPS) spoofing, and replay attack.
  1. Sybil attack means that attackers forged a large number of fake vehicle identities in VANET, this will cause a vehicle in the same VANET to believe the presence of multiple vehicles in the network simultaneously. Sybil attack has a great influence, a hacker gaining access to VANET using Sybil attack may also be able to declare there is no vehicle at one particular position currently. However, the fact is that there is a vehicle at that location, which would cause crash and accident. As a result of Sybil attack, it will disrupt the normal order of the network, as well as disrupt the real-life order, which would threaten the safety of the driver and the road [4,26].
  2. Bogus information attack means that attacker accesses network and sends wrong messages to the vehicle which uses V2V and V2I system. For example, the attacker invades the roadside infrastructure and sends bogus information "slow down" to the yellow car, and sends "the way is clear" to the blue car. In a normal situation, the driver trusts this information, then the attacker most likely succeed in cause the planned accident as the driver would not have enough time to react to it.
  3. In [1], Man in the Middle Attack (MiMA) means that a malicious vehicle eavesdrops on the communication messages in VANET, and injects some wrong information, which can mislead other vehicles in the network.

4. Global Positioning System (GPS) spoofing means that an attacker could modify some of the data to make a wrong GPS data, which misleads drivers and let them think they are in different locations.
5. For replay attack, the attackers reinject the packets which were created before inside the network. Since VANETs essentially need a real-time operating system to support it, the replay attack will upset the networks' order thus to achieve the purpose of affect the network.

– Many threats affect availability: denial of service attack, malware, spamming, black hole attack, and broadcast tampering [1,5,18,27,29].
1. Denial of service (DoS) attacks is an attack which uses network protocol vulnerabilities or uses some illegal means to attack the network. DoS usually creates unprecedented/unexpected fake communication loads for VANETs in a short time to render VANETs impossible to provide normal services thus to achieve the purpose of crashing VANETs.
2. Malware is an attack, which usually originates from vehicles' inside. It might undermine vehicle infotainment systems, ECUs or other mission critical components inside a vehicle causing critical outages.
3. Spamming may make the network transmission speed slower than before. Meanwhile, the spam messages are difficult to control due to lack of centralized management and infrastructure support.
4. Black hole attack is caused by malicious nodes. The malicious nodes can send false information to mislead the network connecting with the vehicle. When the connection is established, the malicious nodes can drop some transmission data, thus resulting in packet loss and transfer failure.
5. Broadcast Tampering is an attack which generates false traffic messages into VANETs and causing significant outages.

3.3 Vehicle Social System Attacks

In the foreseeable future, vehicles will be able to connect to the cloud client via the wireless network or the mobile phone network 3G/4G. According to [10], many vehicle manufacturers including Ford, Nissan, and Toyota have begun to design and develop the vehicle social system (vehicle to cloud). Especially, Microsoft will provide their Azure cloud platform to Toyota which used to provide a cloud solution [10]. This kind of communication can provide vehicle tracking, remotely assistance and emergency relief to the drivers.

As explained in Sect. 2, Vehicle Social System is going to lead the future of vehicle systems. In [10], it is shown that many vehicle manufacturers (i.e., Ford, Nissan, and Toyota) have begun to design and develop the vehicle social system (vehicle to cloud). Especially, Toyota already built a partnership with Microsoft. Microsoft will provide their Azure cloud platform to Toyota which used to provide a telematics cloud solution. This kind of communication can provide vehicle tracking, remotely assistance and emergency relief to the drivers.

However, since drivers can start to share information and experience to cloud client, their privacy information are at risk. For instance, vehicle social system

relies on mobile devices and thus so long as attackers can hack into mobile devices, they can track drivers' location, and steal their personal information.

Moreover, the vehicle to cloud communication is also facing the following challenges: communication latency, gateway, data processing, fleet management, and security [10].

In [10], it is shown the Vehicle Social System is facing the research challenges with communication latency, gateway design, data processing, fleet management, and security. Among these challenges, security and privacy issues are mission critical. Since Vehicle Social Systems, for the first time in this scale in vehicle's history, integrates vehicle systems with other non-vehicle systems to form a big social system, attackers can steal personal information and launch security attacks more easier than ever. Therefore, a wide variety of security and privacy issues must be improved. According to [10], it is necessary to integrate data security and privacy features, and create a cryptography technique which follows certain standards and design efficiency.

4 Related Work

According to the trend of modern vehicle system's development, there are several kinds of modern vehicle systems, such as vehicle networked control system, vehicle infotainment system, vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) system, and vehicle social system. Most recent attacks focus on the inter-vehicle systems.

Luo and Hubaux [22] stated that inter-vehicle communication (IVC) is an important part of Intelligent Transportation System (ITS) and IVC provide communications between driver and driver, or vehicle and vehicle, which can improve the road safety and driving efficiency. Meanwhile, this study simulated the real situation and procided the result of simulation, especially compare between Control Access CDMA (CA-CDMA) and IEEE 802.11. This study covered various aspects of IVC system, which is the strength of the work. But that, unfortunately, this study did not provide any possible solutions of security issues, which is a limitation.

According to Hartenstein and Laberteaux [13], vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) is based on wireless network to build and they contain in vehicular ad hoc networks (VANETs). In addition, the authors provided the main challenge of VANETs, which divided into two parts: technical challenges and socio-economic challenges, such as bandwidth, dynamic network topology and roadside infrastructure etc. The strength of the work is that detailed explanation and introduction were provided in this study, especially the main challenges of VANETs.

Sichitiu and Kihl [33] pointed out inter-vehicle communication (IVC) system can improve the road safety, driving efficiency and comfort of drivers and passengers. Meanwhile, the author showed that the main difference between single-hop system and multi-hop system. Moreover, the author provided the architecture of Vehicular Communications (VC), which include inter-vehicle communications

(IVC), hybrid-vehicle communications (HVC) and roadside-vehicle communications (RVC). The strength of the work is that this survey is a basic study of IVC system. However, the limitation and possible solutions were not presented in this survey, which is the weakness of this work.

Moharrum and Al-Daraiseh [24] pointed out vehicular ad-hoc networks (VANETs) are wireless communication system, which can provide safety and efficient road services to drivers and passengers. In addition, some recent security issues in VANETs were presented in this survey. Meanwhile, several types of attacks and attackers were provided in [24]. The strength of the work is that some solutions which based on current techniques were provided in this study. Another strength is that the authors also pointed out some future challenges and security issues, which still in VANETs.

Most of existing research overlook the applications and inter-connectivity of cyber and physical systems. Due to such limited scope, many attacks across cyber-physical layers are overlooked. Thus, this paper highlights such attacks and arises the awareness of researchers in the field.

5 Conclusions

In conclusion, this paper exposes the fact that security attacks across cyber-physical layers post serious threats to the modern vehicle systems and the users of the system.

We analyze the five different types of modern vehicle systems and the associated security attacks in details. We also list the published attacks which successfully took control of the vehicle or at least the key features related to driving. Some attacks severely endanger the security and safety of the vehicle users; some attacks breach the user's privacy; other attacks may impact both security and privacy. Furthermore, these attacks can be launched from the well researched mobile platforms which lowers the cost of successful attacks and increases the difficulty of securing all vehicles connected to a network. Situations can be worse if there exists a high level of connection such as at the social level, where private travel information can be leaked or misused by malicious attackers.

References

1. Al-Kahtani, M.S.: Survey on security attacks in vehicular ad hoc networks (vanets). In Proceedings of ICSPCS, pp. 1–9. IEEE (2012)
2. Apple. CarPlay (2016). http://www.apple.com/au/ios/carplay/?cid=wwa-au-kwg-features. Accessed 5 April 2016
3. Apple. Siri (2016). http://www.apple.com/au/ios/siri/. Accessed 5 April 2016
4. Boneh, D., Franklin, M.: Identity-based encryption from the weil pairing. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 213–229. Springer, Heidelberg (2001). doi:10.1007/3-540-44647-8_13
5. Brooks, R.R., Sander, S., Deng, J., Taiber, J.: Automobile security concerns. Veh. Technol. Mag. **4**(2), 52–64 (2009)

6. Delgrossi, L., Zhang, T.: Dedicated short-range communications. In: Vehicle Safety Communications: Protocols, Security, and Privacy, pp. 44–51 (2009)
7. Dresner, K., Stone, P.: A multiagent approach to autonomous intersection management. J. Artif. Intell. Res. **31**, 591–656 (2008)
8. Ehsani, M., Gao, Y., Emadi, A.: Modern Electric, Hybrid Electric, and Fuel Cell Vehicles: Fundamentals, Theory, and Design. CRC Press (2009)
9. Etschberger, K.: Controller Area Network: Basics, Protocols, Chips and Applications. IXXAT Press, Weingarten (2001)
10. Faezipour, M., Nourani, M., Saeed, A., Addepalli, S.: Progress and challenges in intelligent vehicle area networks. Commun. ACM **55**(2), 90–100 (2012)
11. Greengard, S.: Automotive systems get smarter. Commun. ACM **58**(10), 18–20 (2015)
12. Gusikhin, O., Filev, D., Rychtyckyj, N.: Intelligent vehicle systems: applications and new trends. In: Cetto, J.A., Ferrier, J.-L., Costa dias Pereira, J.M., Filipe, J. (eds.) Informatics in Control Automation and Robotics. LNEE, vol. 15, pp. 3–14. Springer, Heidelberg (2008)
13. Hartenstein, H., Laberteaux, K.P.: A tutorial survey on vehicular ad hoc networks. Commun. Mag. **46**(6), 164–171 (2008)
14. Hoh, B., Gruteser, M., Xiong, H., Alrabady, A.: Enhancing security and privacy in traffic-monitoring systems. Pervasive Comput. **5**(4), 38–46 (2006)
15. Hoppe, T., Dittman, J.: Sniffing/replay attacks on can buses: a simulated attack on the electric window lift classified using an adapted cert taxonomy. In: Proceedings of WESS, pp. 1–6 (2007)
16. Isaac, J.T., Camara, J.S., Zeadally, S., Marquez, J.T.: A secure vehicle-to-roadside communication payment protocol in vehicular ad hoc networks. Comput. Commun. **31**(10), 2478–2484 (2008)
17. Miller, R., Rouf, I., Mustafa, H., Taylor, T., Oh, S., Xu, W., Gruteser, M., Trappe, W., Seskar, I.: Security and privacy vulnerabilities of in-car wireless networks: a tire pressure monitoring system case study. In: 19th USENIX Security Symposium, pp. 11–13 (2010)
18. Jungels, D., Raya, M., Aad, I., Hubaux, J.P.: Certificate revocation in vehicular ad hoc networks. Technical LCA-Report-2006-006, LCA (2006)
19. Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, D., et al.: Experimental security analysis of a modern automobile. In: IEEE Symposium on Security and Privacy, pp. 447–462. IEEE (2010)
20. Le-Anh, T., De Koster, M.: A review of design and control of automated guided vehicle systems. Eur. J. Oper. Res. **171**(1), 1–23 (2006)
21. Li, Q.: Impacts of vehicle to infrastructure communication technologies on vehicle emissions. Environ. Sci. Technol. **1**, 326 (2014)
22. Luo, J., Hubaux, J.-P.: A survey of inter-vehicle communication. Technical report (2004)
23. Maaroufi, S., Pierre, S.: Vehicular social systems: an overview and a performance case study. In: Proceedings of the Fourth ACM International Symposium on Development and Analysis of Intelligent Vehicular Networks and Applications, pp. 17–24. ACM (2014)
24. Moharrum, M.A., Al-Daraiseh, A.A.: Toward secure vehicular ad-hoc networks: a survey. IETE Techn. Rev. **29**(1), 80–89 (2012)
25. Nilsson, D.K., Larson, U.E.: Simulated attacks on can buses: vehicle virus. In: Proceedings of AsiaCSN, pp. 66–72 (2008)

26. Park, S., Aslam, B., Turgut, D., Zou, C.C.: Defense against sybil attack in vehicular ad hoc network based on roadside unit support. In: Proceedings of MILCOM, pp. 1–7. IEEE (2009)
27. Pawar, T., Manekar, A.: Security threats and its solution for vehicular ad hoc network: a review. Int. J. Electron. Commun. Soft Comput. Sci. Eng. **3**(7), 17 (2014)
28. PRNewswire. PRNewswire (2016). http://goo.gl/ZET6NO. Accessed 5 April 2016
29. Razzaque, M., Salehi, A., Cheraghi, S.M.: Security and privacy in vehicular ad-hoc networks: survey and the road ahead. In: Khan, S., Pathan, A.-S.K. (eds.) Wireless Networks and Security. SCT, pp. 107–132. Springer, Heidelberg (2013)
30. Sangiovanni-Vincentelli, A., Natale, M.: Embedded system design for automotive applications. Computer **40**(10), 42–51 (2007)
31. Schuette, H., Waeltermann, P.: Hardware-in-the-loop testing of vehicle dynamics controllers-a technical survey. Technical report, SAE Technical Paper (2005)
32. Sha, W., Kwak, D., Nath, B., Iftode, L.: Social vehicle navigation: integrating shared driving experience into vehicle navigation. In: Proceedings of the 14th Workshop on Mobile Computing Systems and Applications, p. 16. ACM (2013)
33. Sichitiu, M.L., Kihl, M.: Inter-vehicle communication systems: a survey. Commun. Surv. Tutorials **10**(2), 88–105 (2008)
34. Tashev, I., Seltzer, M., Ju, Y.C., Wang, Y.Y., Acero, A.: Commute UX: voice enabled in-car infotainment system. In: Mobile HCI, vol. 9 (2009)
35. Tegra. Tegra (2016). http://www.nvidia.com/object/tegra.html. Accessed 5 April 2016
36. Tesla. Tesla (2016). https://www.teslamotors.com/en_AU/. Accessed 5 April 2016
37. Toth, P., Vigo, D.: Vehicle Routing: Problems, Methods, and Applications, vol. 18. SIAM, Philadelphia (2014)
38. Verdult, R., Garcia, F.D., Balasch, J.: Gone in 360 seconds: Hijacking with hitag2. In: Proceedings of USENIX Security, pp. 237–252 (2012)
39. Vis, I.F.: Survey of research in the design and control of automated guided vehicle systems. Eur. J. Oper. Res. **170**(3), 677–709 (2006)
40. Xu, Q., Mak, T., Ko, J., Sengupta, R.: Vehicle-to-vehicle safety messaging in DSRC. In: Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks, pp. 19–28. ACM (2004)
41. Yang, X., Liu, J., Vaidya, N.H., Zhao, F.: A vehicle-to-vehicle communication protocol for cooperative collision warning. In: Proceedings of MOBIQUITOUS, pp. 114–123. IEEE (2004)