CTR D-STOP

Technical Report 134

Cybersecurity Challenges and Pathways in the Context of Connected Vehicle Systems

Research Supervisor
Chandra Bhat
Center for Transportation Research

February 2018

Data-Supported Transportation Operations & Planning Center (D-STOP)

A Tier 1 USDOT University Transportation Center at The University of Texas at Austin

CTR CENTER FOR TRANSPORTATION RESEARCH

WNCG Wireless Networking & Communications Group

D-STOP is a collaborative initiative by researchers at the Center for Transportation Research and the Wireless Networking and Communications Group at The University of Texas at Austin.

DISCLAIMER

The contents of this report reflect the views of the authors, who are responsible for the facts and the accuracy of the information presented herein. This document is disseminated under the sponsorship of the U.S. Department of Transportation's University Transportation Centers Program, in the interest of information exchange. The U.S. Government assumes no liability for the contents or use thereof.

Technical Report Documentation Page

1. Report No. D-STOP/2017/134	2. Government Accession No.	3. Recipient's Catalog No.
4. Title and Subtitle Cybersecurity Challenges and Pathways in the Context of Connected Vehicle Systems		5. Report Date February 2018 6. Performing Organization Code
7. Author(s) Enoch R. Yeh, Junil Choi, Nuria G. Prelcic, Chandra R. Bhat, and Robert W. Heath, Jr.		8. Performing Organization Report No. Report 134
9. Performing Organization Name and Address Data-Supported Transportation Operations & Planning Center (D-STOP) The University of Texas at Austin 3925 W. Braker Lane, Stop D9300 Austin, Texas 78759		10. Work Unit No. (TRAIS) 11. Contract or Grant No. DTRT13-G-UTC58
12. Sponsoring Agency Name and Address Data-Supported Transportation Operations & Planning Center (D-STOP) The University of Texas at Austin 3925 W. Braker Lane, Stop D9300 Austin, Texas 78759		13. Type of Report and Period Covered 14. Sponsoring Agency Code
15. Supplementary Notes Supported by a grant from the U.S. Department of Transportation, University Transportation Centers Program.		

16. Abstract

As vehicles become more automated, security issues in automotive systems such as radar and dedicated short-range communication (DSRC) must be thoroughly examined. This report provides an overview and comparison of the inherent security flaws in automotive radar and DSRC technologies. Existing implementations of automotive radar are vulnerable to a spoofing attack from a third party, potentially resulting in fatal accidents. While DSRC exhibits inherent resilience to spoofing attacks, it is still susceptible to similar types of attacks used against traditional Wi-Fi. This report concludes with a discussion on the motivation for combining radar and DSRC into a joint system and an overview of the potential consequences of an insecure vehicular system.

17. Key Words Security risks, automotive radar, DSRC, jamming, spoofing, vehicular networks	18. Distribution Statement No restrictions. This document is available to the public through NTIS (http://www.ntis.gov): National Technical Information Service 5285 Port Royal Road Springfield, Virginia 22161		
19. Security Classif.(of this report) Unclassified	20. Security Classif.(of this page) Unclassified	21. No. of Pages 20	22. Price

Disclaimer

The contents of this report reflect the views of the authors, who are responsible for the facts and the accuracy of the information presented herein. This document is disseminated under the sponsorship of the U.S. Department of Transportation's University Transportation Centers Program, in the interest of information exchange. The U.S. Government assumes no liability for the contents or use thereof.

The contents of this report reflect the views of the authors, who are responsible for the facts and the accuracy of the information presented herein. Mention of trade names or commercial products does not constitute endorsement or recommendation for use.

Acknowledgements

This research was partially supported by the U.S. Department of Transportation through the Data-Supported Transportation Operations and Planning (D-STOP) Tier 1 University Transportation Center. This work was also sponsored by the Texas Department of Transportation under Project 0-6877 entitled Communications and Radar-Supported Transportation Operations and Planning (CAR-STOP). This report under the title of "Security in Automotive Radar and Vehicular Networks" was published in *Microwave Journal*, 60(5), 148-165, May 2017.

.

TABLE OF CONTENTS

Chapter 1. Introduction

Many new radio frequency (RF) technologies are being deployed to make driving safer and more automated. Automotive radar is one such technology, where RF signals are used for adaptive cruise control, forward collision warning, or blind spot detection. Wireless communication used by cars is also increasing. For example, many models support mobile Wi-Fi hotspots. Going forward, many vehicles will be connected using dedicated short-range communication (DSRC), a wireless communications standard that enables reliable data transmission in active safety applications. Each technology, however, comes with its own security risks. Even isolated security breaches could have a dramatic impact on consumer confidence, resulting in the discontinuation of such technologies. In this report, we present an overview and comparison of security risks associated with both automotive radar and DSRC systems. We make a suggestion about how the industry should respond to these known threats, for example, through joint radar and communication. Furthermore, we describe an instance of a past successful attempt to hack a vehicle and speculate on future hacking attempts.

Chapter 2. Security Risks of Automotive Radar

The majority of automotive radars on the market today operate in the millimeter wave (mmWave) band [1]. Figure 1 illustrates the major uses of mmWave radar in vehicles. Specifically, long range radar operates at 76–77 GHz, medium range radar operates at 77–81 GHz, and short range radar operates at 79–81 GHz (was previously at the 24 GHz band). Additionally, research on leveraging the IEEE 802.11ad standard for automotive radar at 60 GHz is currently being conducted at The University of Texas at Austin [2].

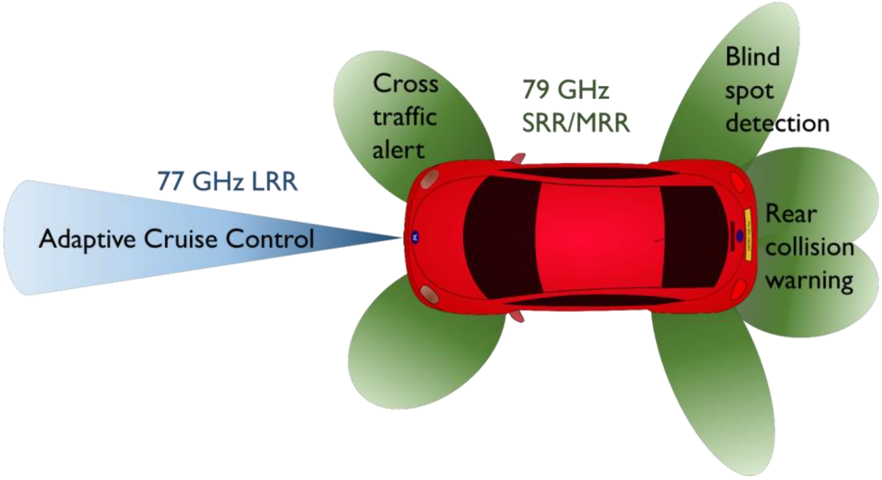

Figure 1. Illustration of all the major uses of mmWave radar in a vehicle.

The types of attacks on vehicular radars are slightly different than the ones targeted on radars in other settings due to the mobile nature of vehicular networks. According to [3], [4], there are three principle attacks (i.e., intentional disruption of a vehicular system by a third-party) on automotive radar. *Jamming* is the transmission of RF signals to interfere with a radar by saturating its receiver with noise. *Spoofing* is the replication and retransmission of radar transmit signals designed to provide false information to a radar to corrupt received data. *Interference* is the intentional or unintentional modification or disruption of a radar signal due to unwanted signals, such as signals from different automotive radars. Note that although some forms of interference may not be considered as an attack, we will discuss their implications for the sake of completeness

2.1 Jamming

Figure 2 illustrates two different types of attacks as a result of jamming. Both forward and blind spot jamming attacks can effectively disable the functionality of vehicular radar, leaving the driver vulnerable to a collision. Due to the long-term use of mmWave radars in military applications, there has been an [3], [5]. A simple jamming technique uses a tunable scanner to determine the frequency of a radar signal and generates a jamming signal at the same frequency, disrupting the target radar's receivers [6]. More advanced jamming techniques may exploit transmitting jamming signals on specific polarizations to more effectively disrupt the target radar's antennas [7], [8].

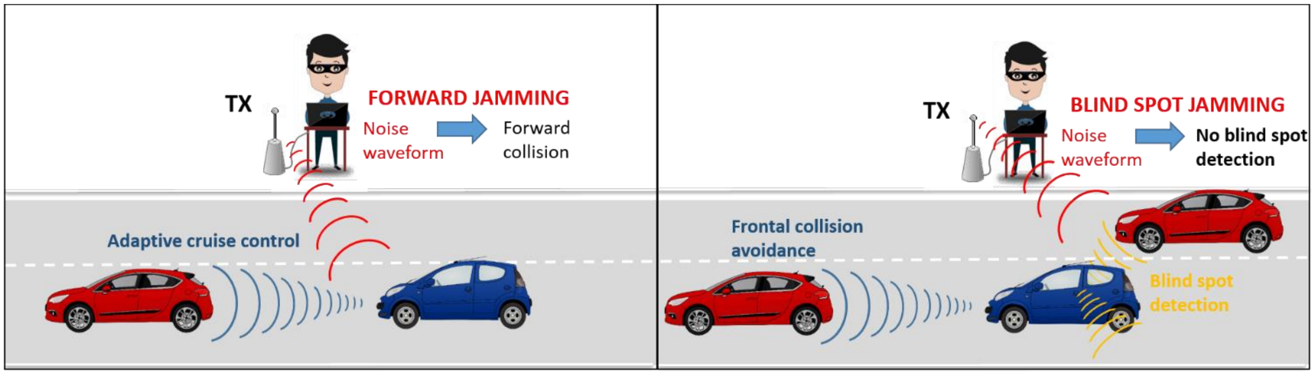

Figure 2. Illustration of two different types of attacks as a result of jamming.

Automotive mmWave radar experiences limited range due to the small wavelength and inability to pass through solid objects consistently [9]. Most radars use a substantial amount of directivity in the system to overcome this effect. This gives automotive mmWave radar more resistance to jamming compared to devices that operate at low frequencies. Additionally, since the purpose of jamming is to deny the victim service, it is moderately difficult to perform an effective jamming attack on an automotive radar in a highly mobile environment.

If the jammer has a static location, even a successful breach will disrupt the automotive radar for as long as the target is in range, which could be a matter of a few seconds in highly mobile environments (i.e., highways). Although the potential consequences of losing a few seconds of operation are significant (i.e., loss of collision detection for that time frame), it is incredibly difficult for a malicious attacker to predict exactly where and when the jammer needs to operate to cause an accident. As a result, the attacker is limited to jamming in environments with low mobility (i.e., downtown areas) and does not have the ability to focus an attack on a single radar system.

If the jammer is mobile, much more damage can inflicted. A jammer located on a vehicle that is currently following the target may be able to continuously jam the target. Executing a continuous jamming attack requires two major components to be successful. First, the vehicle with the jammer must stay within a certain range of the target vehicle without attracting suspicion to itself. Second, the operation requires a jammer that can accurately scan the wireless channel in a highly mobile environment, which is notably complex. To perform the attack, the jammer must be able to scan the target vehicle from any direction and distinguish the target vehicle’s radar signals from any other wireless signal. It must also transmit a strong jamming signal in the direction of the target vehicle.

Overall, although jamming attacks have the potential for inducing major collisions in the future, current jammers do not have the necessary adaptability for performing in a highly mobile environment, making it very difficult for malicious attackers to target a single vehicle.

2.2 Spoofing

Automotive mmWave radars are known to be susceptible to spoofing, the replication and retransmission of radar transmit signals to introduce false information and corrupt received data. Figure 3 illustrates an attack on a mmWave radar as a result of spoofing, which has the potential to cause the radar to report false information and greatly increases the risk of a collision. A spoofing demonstration was presented in [10], where the target radar reported distances significantly shorter than the distance of the actual target. In addition, distance and velocity-falsifying attacks on commercial automotive radars have been shown to be feasible [10], [11].

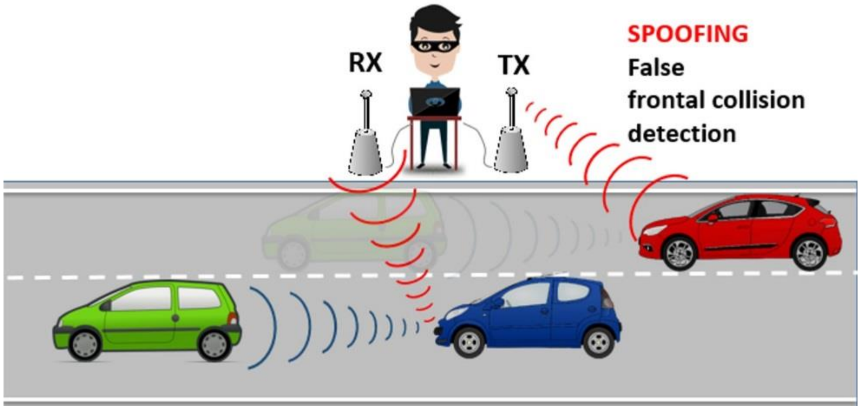

Figure 3. Illustration of an attack as a result of spoofing.

Automotive radar exploits a specific signal structure that performs well as a radar signal (i.e., has strong autocorrelation properties) but exhibits no inherent authentication, leaving it vulnerable to spoofing attacks. Without a means for checking signal integrity, the receiver is unable to verify the spoofed sequences, making it possible to analyze and replicate the signal. Unlike a jamming attack, a spoofing attack is designed to confuse the target victim. Ideally, a spoofing attack only needs to breach the target radar for a short period of time to severely influence the behavior of the target vehicle, potentially causing it to stop, change direction, or in the worst case, collide. Based on this, a successful spoofing attack can have a devastating effect on automotive radars on the market today. Despite this, there has been no publicized report of a spoofing attack on a vehicle. We believe that this is due to the relatively high implementation complexity of designing an effective and robust spoofing system. Overall, spoofing is the primary security concern for automotive radar due to its potential consequences and feasibility.

2.3 Interference

Most automotive radars are frequency-modulated continuous wave (FMCW) radars [12]. These radars exploit small shifts in signal frequency, by transmitting a signal that varies in frequency over a fixed period of time. This technique provides a speed measurement along with a distance measurement, further refining the accuracy of automotive radars. Since the receivers of these radars expect a signal with a definitive frequency pattern, it can perform more advanced signal cancellation techniques to reduce the effect of interference (including jamming) [13]. Despite this inherent advantage, there are some forms of interference, such as a chirp or sweep signal, that cannot be isolated as detailed in [14], resulting in performance degradation in the presence of heavy interference. Due to the limited use of automotive radar, interference is not a problem in vehicular environments today. As automotive radars become more widespread, however, we predict that interference between automotive radars of different vehicles will become a major issue.

Chapter 3. Security Risks of DSRC

In 2017, several newly released vehicles will use DSRC technologies to communicate over designated vehicular networks in the U.S. These networks enable mobilized vehicles to exchange data with other vehicles (vehicle-to-vehicle, or V2V) as well as infrastructure (vehicle-to-infrastructure, or V2I) within range. Information such as velocity and global position can be used by V2V applications that leverage DSRC to perform collision prevention and driver assistance tasks, making it extremely important that DSRC devices be reliable and secure. Additionally, V2I applications that use DSRC can provide more convenient e-parking, vehicle safety inspection, and toll payment services. In general, DSRC exhibits low network latency, high reliability, a priority ranking hierarchy, and improved security and privacy [15].

Current implementations of vehicular communication systems are modeled after existing Wi-Fi communication systems (i.e., IEEE 802.11p, the standard used in DSRC, is a subset of the IEEE 802.11 standard). Thus, in general, DSRC technologies are susceptible to similar types of attacks used against traditional Wi-Fi, which include jamming, spoofing, and interference [16]. In addition to these attacks, DSRC technologies are also susceptible to attacks on user confidentiality.

3.1 Jamming

In contrast to automotive mmWave radar, DSRC devices operate at relatively low frequencies of 5.9 GHz, improving its maximum range of detection but making it more susceptible to jamming attacks. Research has shown that constant, random, and intelligent jamming attacks can deny service to DSRC applications to the point of disabling their entire functionality [17]. In addition, DSRC may potentially experience denial-of- service attacks designed to jam the system from within the vehicular network, such as malware, spamming, and black hole attacks [16]. All these attacks have the potential to disable vehicular communications for an extended period of time, putting the targeted vehicle and its occupants in danger if the vehicle relies on DSRC for collision warning.

To combat these potential attacks, considerable research has examined solutions such as implementing additional authentication, physically separating networks within the same vehicle, switching frequencies when denied service, and communicating with legitimate DSRC devices to blacklist rogue devices [17]–[19]. Despite these efforts, jamming is still a major security concern for DSRC systems due to the ease of carrying out an attack and the potential consequences it has on targeted systems.

3.2 Spoofing

Although DSRC is more susceptible to jamming than automotive radar, it exhibits inherent resistance to spoofing attacks. Since DSRC is a subset of the IEEE 802.11 standard, it has a predefined packet sequence that incorporates packet authentication within its packet headers. Due to this, spoofing a DSRC device requires knowledge of the specific sequences used in the packet headers. In addition, the DSRC standard is capable of incorporating public key cryptography during transmission, further improving the security of these devices.

Despite these advantages, DSRC is still vulnerable to specific types of spoofing attacks. These include attacks from within the network itself and attacks that modify the signals sent throughout the network. If the attacker is able to somehow determine or obtain the necessary credentials for authentication, then it may be able to impersonate a legitimate device, enabling the attacker to send false information to the target device [20]. In contrast, spoofing attacks such as replay attacks or man-in-the-middle attacks may allow an adversary to modify signal information by intercepting a transmitted signal and retransmitting a slightly modified version of the signal. Overall, although DSRC technology is ultimately susceptible to spoofing, its inherent robustness due to predefined packet authentication mitigates the severity of this security risk. Furthermore, several supplementary measures can be implemented to provide additional security such as additional authentication.

3.3 Interference

DSRC has been allocated a 75 MHz frequency band at 5.9 GHz by the Federal Communications Commission. Due to this, DSRC does not experience any (legal) interference from non-DSRC devices, such as Wi-Fi devices that operate at the 5 GHz band. Currently, there are relatively few DSRC devices implemented in vehicles on the road, rendering interference as a non-issue. In the future, however, when DSRC devices become widespread, interference between mutual devices will be a concern, especially in congested environments such as downtown areas. Although current strategies for reducing mutual interference (such as interference cancellation, power and frequency adaptation, and improved MAC layer protocol design) can decrease the effect of interference on DSRC, mutual interference is still a notable security concern that has yet to be completely addressed [21], [22].

3.4 Confidentiality

In addition to jamming, spoofing, and interference, DSRC devices must also address the issue of confidentiality due to its nature as a communications system. Not only do DSRC devices need to maintain information privacy, but they also need to ensure that unwanted third parties cannot covertly track the location of the device over an extended period of time. Potential threats to confidentiality include eavesdropping, masquerading, and traffic analysis [23].

Although the consequences of failing to address information and location privacy are not as severe compared to those of jamming, spoofing, and interference, maintaining confidentiality is one of the more discussed security topics in vehicular networks. This is due to the exceptionally low complexity of conducting an attack on confidentiality. For naïve DSRC technologies, such attacks can be performed by listening to the data transmissions within a network and analyzing the traffic. Furthermore, even if the data itself is encrypted, modern traffic analysis techniques can examine traffic patterns of a specific device and extract location information from the analysis. As a result, DSRC technologies need to be designed intelligently in order to prevent attacks on confidentiality. Currently, there are various measures for preventing attacks on confidentiality such as device cloaking; however, these solutions introduce considerable complexity to the entire network and are sometimes undesirable.

Chapter 4. Comparing Automotive Radar and DSRC Security

In summary, both automotive radar and DSRC technologies have inherent security flaws as summarized in Table 1. On the one hand, DSRC devices are more susceptible to jamming than automotive radars since they are subject to jamming attacks from within the vehicular network. On the other hand, automotive radars are considerably more susceptible to a spoofing attack than DSRC technologies due to their lack of signal verification. Currently, both automotive radar and DSRC devices are not significantly impacted by interference. In the future, when the technologies become more widespread, interference will become an important security concern that needs to be addressed. In addition, DSRC technology must account for attacks on confidentiality due to its nature as a communications system. Overall, although there are more types of attacks on DSRC systems, DSRC is more secure than automotive radar due to its built-in security mechanisms and its ability to communicate with other legitimate DSRC sources. This does not mean that DSRC equivalents can replace automotive radar, since the functionalities of both technologies are crucial for a variety of vehicular applications.

Table 1. Security Comparison between Automotive Radar and DSRC

	Automotive Radar	**DSRC**
Jamming	Moderate	High
Spoofing	High	Moderate
Interference	Low	Low
Confidentiality	None	Moderate

‘High’ indicates a security risk with a high potential for major consequences,
‘Moderate’ indicates a security risk with a moderate potential for major consequences or a high potential for minor consequences,
‘Low’ indicates a security risk with a small potential for both major and minor consequences, and
‘None’ indicates no security risk.

At The University of Texas at Austin, we are performing research on joint radar and communication. One line of research is to fuse information derived from separate radar and DSRC modules. As shown in [24], [25], this can improve target localization. In addition, a joint system is not solely dependent on a single factor, such as sensor quality or degree of noise. Furthermore, while the DSRC aspect of the system remains the same, the radar aspect receives an extra layer of authentication, dramatically reducing the device’s vulnerability towards a spoofing attack. Joint radar and communications devices either operate using the same signal or different time/frequency resources, which does not increase the effect of mutual interference on the system.

One of our primary areas of research is how to incorporate a communications waveform (e.g., IEEE 802.11ad) and its inherent security into the signal structure of automotive radar [2]. By exploiting special data sequences within the IEEE 802.11ad signal structure, radar parameter estimation for both range and velocity detection can be performed with high accuracy. This framework enables joint long-range automotive radar and vehicle-to-vehicle communication at 60 GHz, improving detection accuracy and reliability.

Another primary area of research is developing a cost-effective microwave IEEE 802.11p radar that may be used in tandem with automotive radars to perform a security check with the received radar waveform [25]. By exploiting a special characteristic of the IEEE 802.11 channel energy, range detection using a communications waveform at microwave frequencies can be performed at meter-level accuracy. The main advantage of performing radar tasks at microwave frequencies is the significantly reduced cost and increased availability of microwave equipment. In addition, by supporting high-accuracy automotive radars with a joint microwave radar and communications system, the security issues of automotive radar (e.g., spoofing) can be eliminated.

Chapter 5. Hacking a Vehicle

In 2014, security researchers published a paper describing a strategy for a remote automotive attack at an international hacker convention [26]. A year later, they took a step further and demonstrated a wireless attack on a Chrysler Jeep being driven on a public highway, posting the footage in a YouTube video [27]. By exploiting a major oversight in Chrysler's network design, they were able to brute force their way into the system and exploit the Linux operating system. From there, they were able to remotely control steering at low speeds, engine status, the air conditioning system, and radio from the Internet.

Upon the release of the video, the public reacted quite negatively towards this demonstration. Their angry complaints prompted several changes in the automotive industry, one of them being the release of a best practices paper by Intel (McAfee) [28]. This paper outlines all the known ways vehicles can be hacked and the most effective countermeasures, including but not limited to attacks from wireless vehicle-to-vehicle and vehicle-to-infrastructure receivers, Bluetooth systems, and the engine control unit.

Despite the paranoia caused by the video, wireless malicious hacking of a vehicle has been virtually nonexistent. Though the idea has been popularized in movies (such as Disney®'s Tron) or video games (such as Ubisoft®'s Watch Dogs), there has only been one documented instance of malicious hacking of a car. In 2010, an angry former employee bricked hundreds of cars at a dealership [29], [30], destroying several million dollars' worth of cars, but injuring no one in the process. Additionally, although [26] provided a substantial list of vehicle models susceptible to the same type of attack they performed, there have been no reported attacks on any of these vehicles.

This recent public outburst can be explained by the heavy consequences of allowing vulnerable vehicles to drive on public roads. Although the threat of hacking vehicles is real, with the proper precautions, these threats can be avoided altogether. Like any other networking protocol, vehicular networks will always be subject to attack. But as long as security concerns are addressed in an ethical, appropriate, and timely manner, there is no reason to prevent or delay the integration of communication networks in vehicles.

Chapter 6. Conclusions

As automotive radar and vehicular networks grow more and more widespread, it is crucial that the security risks of each technology are examined and addressed. Automotive radar and DSRC technology both exhibit inherent security flaws, motivating the development of a joint radar and communications system. In addition, a documented instance and demonstration of hacking a vehicle on the road has greatly increased public awareness on the topic. Although the security breach demonstrated was not due to the flaws of automotive radar or DSRC technology, it more than sufficiently demonstrated the potential of an attack causing severe consequences.

To perform many of the attacks introduced in this paper, attackers only need to attach a device that can intercept and/or scan a signal to a centralized computer, and in some cases, a signal generator and transmitter. Some of the more complicated attacks mentioned (such as spoofing a DSRC device) may require much more sophisticated equipment that enables the attacker to get access to well-protected information. Due to this, the majority of malicious hackers will likely aim to find a simplistic security breach that allows them to gain considerable access, like the hacking demonstration presented in Section 5. Due to cost and complexity, many hackers will likely avoid attacking a vehicular system using a sophisticated strategy. As black hat research advances, however, conducting spoofing attacks on automotive radar will become more and more feasible, encouraging more malicious hackers to consider spoofing and dramatically increasing the risk of leaving unprotected devices in vehicular environments. The observations presented in this paper should be considered as a sober warning to automobile companies, motivating them to address the security risks of both automotive radar and DSRC technologies as soon as possible.

References

[1] R. Heath Jr., “MIMO at millimeter wave,” https://web.stanford.edu/~apaulraj/workshop70/pdf/mmWaveMIMO_Heath.pdf, 2015.

[2] P. Kumari, N. Gonz´alez Prelcic, and Jr. R. W. Heath, “Investigating the IEEE 802.11ad standard for millimeter wave automotive radar,” in *Proceedings of the Vehicular Technology Conference*, 2015.

[3] N. Currie and C. Brown, *Principles and Applications of Millimeter-wave Radar*, Artech House, 1987.

[4] “Millimeter wave radar brings international recognition,” http://www.gtri.gatech.edu/history/innovations/millimeter-wave-radar-brings-international-recognition, 2011.

[5] N. Li and Y. Zhang, “A survey of radar ECM and ECCM,” *IEEE Trans. Aerospace and Electronic Systems*, vol. 31, no. 3, pp. 1110–1120, 1995.

[6] S. Janusas, “Monopulse radar jammer using millimeter wave techniques,” 1993, US Patent 5200753 A.

[7] X. Qiao, T. Jin, X. Qi, M. Zhang, S. Yuan, and Q. Zhang, “Anti-millimeter wave polarization agile active jamming,” in *Proceedings of the International Conference on Microwave and Millimeter Wave Technology*, 2007, pp. 1–4.

[8] W. Zhang, H, Zeng, Y, Li, and X. Wang, “Polarimetric radar performance test of signal processing for anti-active jamming,” in *IET International Radar Conference*, 2009, pp. 1–4.

[9] V. Richard, *Millimeter wave radar applications to weapons systems*, USA Ballistic Research Laboratories, 1976.

[10] R. Chauhan, “A platform for false data injection in frequency modulated continuous wave radar,” http://digitalcommons.usu.edu/cgi/viewcontent.cgi?article=4983&context=etd, 2014.

[11] S. Roome, “Digital radio frequency memory,” *Electronics & Communication Engineering Journal*, vol. 2, no. 4, pp. 147–153, 1990.

[12] J. Zhao, G. Zucchelli, and M. Roggero, “Design of FMCW radars for active safety applications,” http://embedded-computing.com/articles/design-fmcw-radars-active-safety-applications/, 2015.

[13] A. Stove, “Linear FMCW radar techniques,” *IEEE Radar and Signal Processing*, vol. 139, pp. 343–350, 1992.

[14] M. Brooker, “Mutual interference of millimeter-wave radar systems,” *IEEE Transactions on Electromagnetic Compatibility*, vol. 49, pp. 170–181, 2007.

[15] “DSRC: the future of safer driving,” https://www.its.dot.gov/factsheets/dsrc_factsheet.htm, 2015.

[16] C. Laurendeau and M. Barbeau, “Threats to security in DSRC/WAVE,” in *Proc. 5th International Conference on Ad-Hoc Networks & Wireless, LNCS 4104*, 2006, pp. 266–279.

[17] A. Serageldin, H. Alturkostani, and A. Krings, “On the reliability of DSRC safety applications: a case of jamming,” in *International Conference on Connected Vehicles and Expo*, 2013, pp. 501–506.

[18] T. Zhang, H. Antunes, and S. Aggarwal, “Defending connected vehicles against malware: challenges and a solution framework,” *IEEE Internet of Things Journal*, vol. 1, pp. 10–21, 2014.

[19] H. Hasbullah, I. Soomro, and J. Ab Manan, “Denial of service (DOS) attack and its possible solutions in VANET,” *International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering*, vol. 4, no. 5, pp. 813–817, 2010.

[20] E. Hamida, H. Noura, and W. Znaidi, “Security of cooperative intelligent transport systems: standards, threats analysis and cryptographic countermeasures,” *Connected Vehicles, V2V Communications, and VANET*, vol. 4, no. 3, pp. 380–423, 2015.

[21] S. Maddio, A. Cidronali, M. Passafiume, G. Collodi, and G. Manes, “Interference cancellation for the coexistence of 5.8 GHz DSRC and 5.9 GHz ETSI ITS,” in *IEEE MTT-S International Conference on Microwaves for Intelligent Mobility*, 2015, pp. 1–4.

[22] Q. Xu, T. Mak, J. Ko, and R. Sengupta, “Vehicle-to-vehicle safety messaging in DSRC,” in *Proceedings of the 1st ACM International Workshop on Vehicular ad hoc Networks*, 2004, pp. 19–28.

[23] Information Resources Management Association, *Transportation Systems and Engineering: Concepts, Methodologies, Tools, and Applications*, IGI Global, 2015.

[24] Q. Chen, T. Roth, T. Yuan, J. Breu, F. Kuhnt, M. Zollner, M. Bogdanovic, C.Weiss, J. Hillenbrand, and A. Gern, “DSRC and radar object matching for cooperative driver assistance systems,” in *IEEE Intelligent Vehicles Symposium*, 2015, pp. 1348–1354.

[25] R. C. Daniels, E. R. Yeh and R. W. Heath, "Forward Collision Vehicular Radar With IEEE 802.11: Feasibility Demonstration Through Measurements," in *IEEE Transactions on Vehicular Technology*, vol. 67, no. 2, pp. 1404-1416, Feb. 2018.

[26] C. Miller and C. Valasek, “A survey of remote automotive attack surfaces,” in *DEF CON*, 2014.

[27] “Hackers remotely kill a jeep on the highway-with me in it,” https://www.youtube.com/watch?v=MK0SrxBC1xs, 2015.

[28] “Automotive security: best practices: recommendations for security and privacy in the era of the next-generation car,” http://www.mcafee.com/us/resources/white-papers/wp-automotive-security.pdf, 2015.

[29] “Hacker disables more than 100 cars remotely,” http://www.wired.com/2010/03/hacker-bricks-cars/, 2010.

[30] “Hackers can now hitch a ride on car computers,” http://www.latimes.com/business/autos/la-fi-hy-car-hacking-20150914-story.html, 2015.