计算机体系结构

小综述报告

2019 ~ 2020 学年 第 一 学期

学　　院　信息科学与工程

专　　业　网络空间安全

学　　号　S191000882

姓　　名　唐志泉

无人驾驶车的传感器安全和防御

摘要

无人驾驶汽车（AVs）提供更精确的控制来释放驾驶员的负担的同时也能减少交通事故的发生，从而极大地提高驾驶的便利性。随着人工智能的快速发展和物联网技术的重大进步，我们见证了近年来自动驾驶的稳步发展。尽管前景广阔，但自动驾驶技术的发展也面临着新的挑战，其中安全性是头等大事。本文从传感器的角度对围绕自动驾驶的安全威胁进行了系统的分析。除了对这些威胁的深入概述之外，本文还总结了相应的防御策略。

介绍

近年来，随着人工智能（AI）和物联网（IoT）技术的普及，自动驾驶技术得到了稳步改进，并且越来越多的智能技术可以精确感测现实世界中的环境，快速分析传感器数据以及自主做出复杂的决定。在可预见的未来，AV 被广泛认为是人们日常生活中最受普遍的 AI 应用之一。

尽管前景广阔，但自动驾驶技术的快速发展也面临着新的挑战，其中安全性是头等大事。众所周知，AV 通常配备各种功能丰富的传感器，例如摄像机，雷达，GPS 等，以感知周围的环境。诸如 GPS 之类的各种传感器，超声波传感器，LiDAR（激光）雷达，MMW（毫米波）雷达，都是 AV 不可缺少的“眼睛”。 图 1 显示了无人驾驶车的

一般结构，图 2 显示了嵌入在 AV 中的传感器，表 I 显示了这些传感器的一般描述以及它们的相应使用场景。

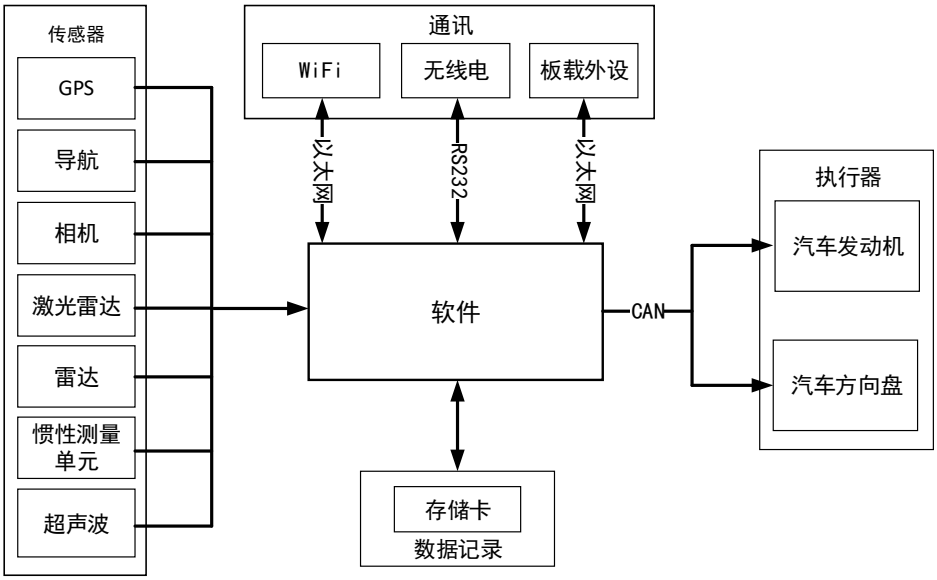

图 1 无人驾驶车的一般结构

配备传感器的自动驾驶汽车可以实现环境感知，避免碰撞，障碍物/行人识别，导航等。考虑到对传感器的高度依赖，一旦传感器“失明”，甚至受到控制，可能导致致命的灾难。在本文中，我们将介绍针对 AV 中最常见传感器的各种类型的攻击，并提供一些相应的防御策略。

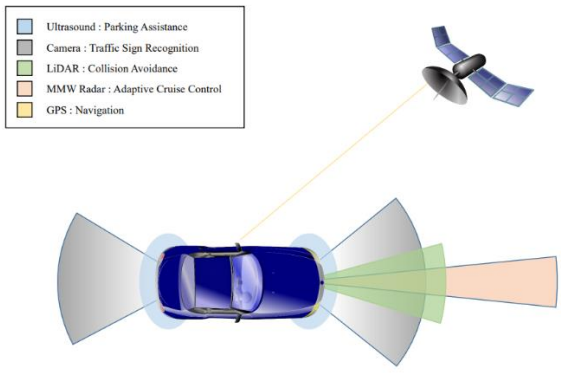

图 2 嵌入在 AV 中的传感器

表 I 传感器的一般描述以及使用场景

传感器	信号	场景	被动/主动	使用

GPS	微波	全球	被动	导航
激光雷达	红外激光	中距离	主动	行人检测 碰撞避免
毫米波雷达	微波	长距离	主动	碰撞避免 自适应巡航控制
超声波雷达	超声波	靠近	主动	停车辅助
摄像头	可视光	短距离	被动	红绿灯识别 车道线检测 障碍物检测

GPS

在过去的十年中，对 GPS 的攻击进行了广泛的研究[1] – [7]。 现有的攻击，例如[2]，[5]，[8]，[9]，证明了 GPS 攻击是可行的。 GPS 攻击主要有两种：欺骗和干扰。由于 GPS 通信的距离较长，来自卫星的 GPS 信号较弱[2]，因此通过使用更强的相同频率信号很容易执行干扰攻击。在下一部分中，我们将重点介绍欺骗性攻击，因为它们比干扰更具威胁性。

8 后，攻击者发送了一个非常强大的伪信号来接管卫星的信号[2]。由于受害者的 GPS 会丢失信号或突然发生变化，因此可以检测到这种攻击[3]。更复杂的策略需要攻击者更加耐心[3] [6][7]。为了对受害者发动攻击，攻击者的虚假信号应与卫星发出的信号同步。同步后，攻击者会增加虚假信号的功率，从而使受害者的 GPS 锁定虚假信号。之后，攻击者可以通过更改伪信号来操纵受害者的位置。其他高级策略，如调零，通过相应地发射负信号来消除 GPS 信号[4]，也可以用于隐身攻击。

在上述攻击策略中，他们主要集中于如何接管受害者的 GPS 信号。Zeng 等人提出的近期攻击[5]，他们制作了如图 3 所示的设备，当受害

者使用导航系统时，利用伪造位置来引导受害者车辆驶入预定位置。驾驶员参与时可能会捕获到这种攻击，但是对于无人驾驶的 AV 来说效率更高。

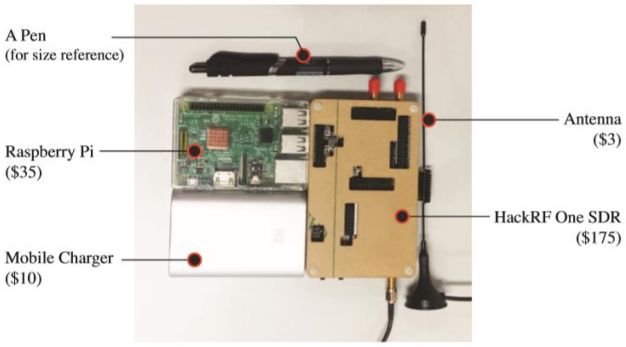

图 3 手工制作能攻击 GPS 信号的设备

为了防止 GPS 定位攻击，人们提出了许多对策。例如，杂散信号看起来与卫星发射的信号不同。我们可以利用这个观测来识别 GPS 攻击。

其他工作[12]-[16]检查到达方向（DoA）。如图 4 所示，它使用天线阵列来减轻攻击，因为 GPS 信号的 DoA 将显示出与欺骗信号不同的进位相位。其他方法将密码技术引入 GPS 信号中，用于攻击防御。O'Hanlon 等人[30]建议加密 GPS L1 P(Y)码以判断是否发生欺骗攻击。认证策略[18]、[19]可用于确保信号的真实性，例如在卫星信号中嵌入签名的导航消息认证（NMA）。

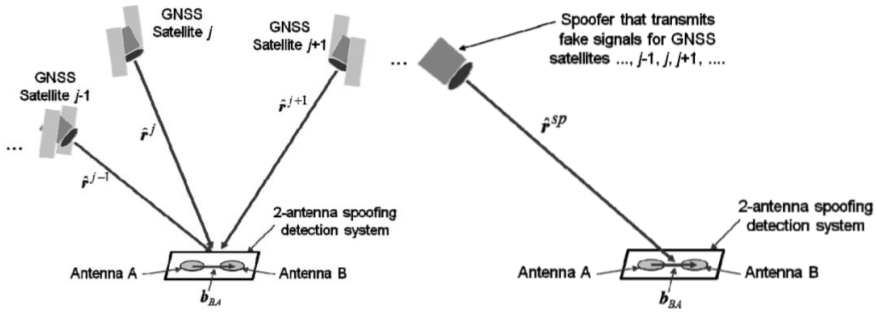

图 4 检测 GPS 信号的到达方向

此外，也可以结合不同研究领域的工作来实现保护，例如距离限

制协议[24]、[25]，该协议可以通过加密工具测量和确保实体之间的距离，或者通过比较当前位置的道路标志或建筑物来计算机视觉技术。

激光雷达

LiDAR 是一种主动感应设备，与摄像头相比，它可以整天工作，而无需考虑光照条件。由于这些基础设施具有反光表面，因此它也可以用于识别标志、车道等[26]凭借这些优势，除特斯拉外，几乎所有的 AV 都配备了 LiDAR，以进行环境感知[20]。LiDAR 通过旋转收发器和发射红外激光来感应周围的障碍物。然后，它通过测量反射激光的往返时间来计算障碍物的距离（如图 5 所示）。现有工作表明，LiDAR 容易受到故意攻击。

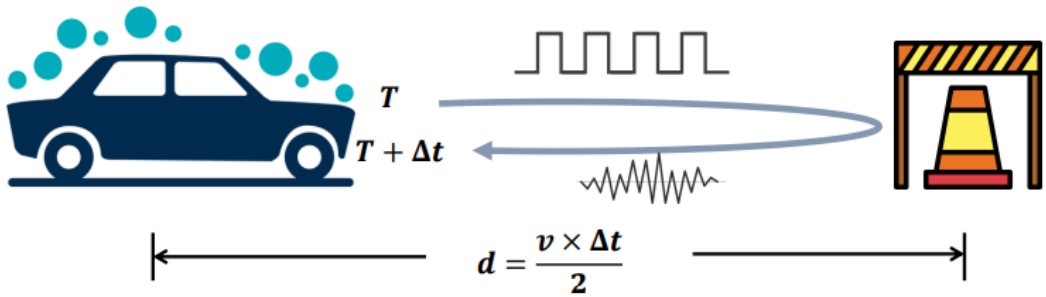

图 5 传感器的工作原理是利用信号的往返时间来计算距离。 在此，v 是空气中信号的速度（例如声音：340m / s，电磁波和光：3×108m / s）。

在 Black Hat Europe 2015 中，Petit 等人[21]首先介绍了针对 AV 中嵌入的 LiDAR 的攻击。在攻击中，攻击者使用收发器接收从 LiDAR 发送的激光脉冲，然后将接收到的信号中继到另一个收发器，该收发器将杂散信号在预定的时间间隔内延迟后将其发送回 LiDAR。通过控制延迟的时间间隔和发送虚假信号的频率，它们的攻击可以实现在固定位置注入多个障碍物。后来，申等人[20]扩大了 Petit 的攻击力，

可以向其注入更近的假障碍。他们利用了 LiDAR 的特性，它通过旋转的激光收发器扫描环境，并且观察到光的传播比 LiDAR 的旋转速度快得多。具有此特征的攻击者可以预先接收激光脉冲，然后立即将激光脉冲中继到 LiDAR 其他角度的另一个收发器。这使攻击者可以比他更靠近伪造的障碍。他们还通过向 LiDAR 发送相同频率的激光来引入干扰攻击。

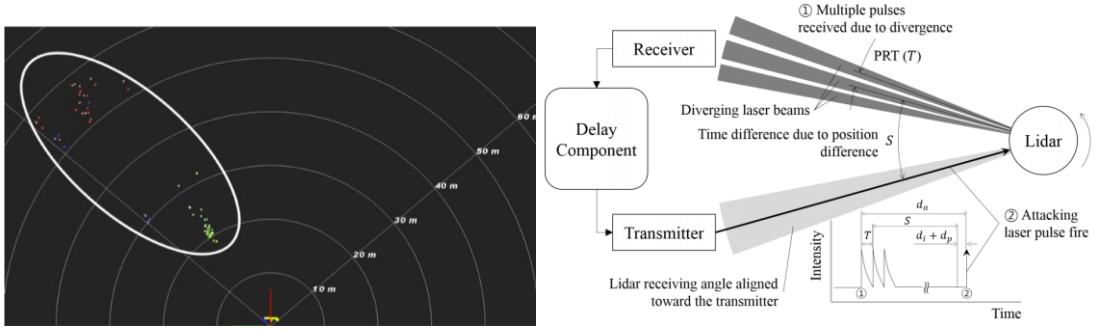

图 6 针对激光雷达的中继攻击和注入攻击

为了抵抗针对激光雷达的攻击，[20]，[21]中的作者列出了以下防御策略。

改变激光雷达发射和接收激光的方式是一种很有前途的方法。如果攻击者想成功执行攻击，则应将假激光与激光雷达的激光同步。向一个方向多次发射激光脉冲（大约三次）对与激光雷达的激光不同步的攻击者是有效的。此外，由于激光雷达在旋转过程中只接受特定角度的激光，因此减小接收角度可以减轻攻击的影响，但这也是激光雷达灵敏度的权衡[27]。

另一个对策是减少激光雷达的接收时间，这将减少激光雷达的探测范围。为确保确定性，激光雷达定义了接收时间，在此时间内激光

雷达接收传入的激光。缩短接收时间会减少攻击者执行攻击的机会，但也会使从远处物体反射的激光失效。另一个策略是在激光雷达工作时引入随机性。考虑到 LiDAR 会使收发机围绕扫描环境旋转，使 LiDAR 以随机速度旋转，并向随机方向发射激光，可以防止[20]提出的攻击。另外，通过发射随机信号或以随机脉冲间隔发射信号，使激光雷达的激光更加不可预测，是对付攻击者的有效方法。

最后，激光雷达的冗余或多传感器融合允许 AV 校正激光雷达的读数。它增加了攻击者的成本和复杂性，同时也由于安装新设备而给客户带来了额外的成本。此外，在非重叠区域，攻击仍然可以发动[20]。

毫米波雷达

MMW 雷达的工作原理与 LiDAR 非常相似，如图 5 所示，除了它发出的信号。MMW 雷达发射的微波波长比 LiDAR 发射的激光更长[28]。与 LiDAR 相比，MMW 雷达不受恶劣天气的影响，例如暴风雨，大雾和灰尘[29]。但是，由于 MMW 雷达的波长更长，因此 MMW 雷达具有较低的分辨率和较短的可检测范围。目前，MMW 雷达已安装在 Tesla 的车辆中。在 DEF CON 2016 中，Yan 等人演示了利用 MMW 雷达[22]的漏洞对特斯拉 Model S 的实际攻击。他们对干扰攻击进行实验，将相同的波形信号发送到 MMW 雷达，以降低信噪比（SNR），从而通过仔细调制类似于 MMW 雷达的信号，成功地发起了欺骗攻击。在他们的研究中，他们得出的结论是，实验结果非常出色，尤其是当 Tesla 在自动驾驶模式下工作时。至于仅依靠毫米波雷达来实现

障碍物识别和避撞的自动驾驶汽车，确实是一个微不足道的威胁。

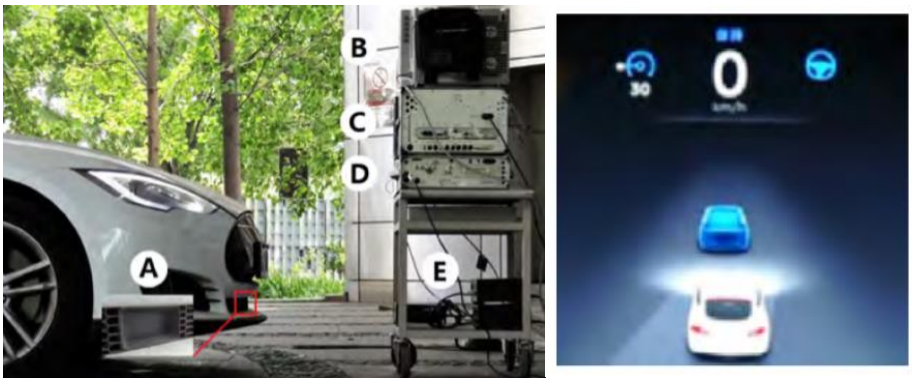

图 7 针对特斯拉 Model S 的欺骗攻击从而产生汽车障碍物

[22]中的作者讨论了如何对抗对雷达的攻击。首先，他们认为干扰攻击很容易被发现，因为现实世界中很少出现类似干扰的信号。当雷达探测到这种信号时，很有可能雷达受到攻击。然后，为了抵抗欺骗攻击，他们建议在雷达信号中引入随机性。最后，他们提出了传感器融合策略，即使用不同的传感器读数互相校正。

超声波传感器

超声波传感器发送和接收超声波，它利用反射的超声波脉冲的传播时间来计算到最近障碍物的距离（见图 5）。通常，大多数人无法感觉到频率高于 18 kHz 的声音。在自动驾驶汽车中，此功能使超声波传感器可用于自动或半自动停车。同样，欺骗和干扰是威胁超声波传感器的两种攻击。

欺骗攻击试图利用精心制作的超声波来制造伪造的障碍物。在[22]中，当在检测范围内没有真实障碍物时，欺骗攻击会造成伪障碍。相反，如果障碍物更多，这种攻击很容易在 AV 的决策过程中引起混乱。除了这项工作之外，在[23]中，Xu 等人通过创建针对现成的传感器以

及 AV 配备的机载传感器的假想障碍，进一步演示自适应欺骗攻击。

干扰攻击是一种较为简单但仍具有威胁性的方法，旨在通过连续发射超声波来降低超声波传感器的 SNR。在[22]，[23]中，对奥迪、大众、特斯拉和福特进行了测试，结果表明，干扰攻击会误导汽车，同时驾驶员将不会收到有关障碍物的任何警告。 [23]中的另一项实验表明，在自动停车模式和传唤模式下，干扰攻击对特斯拉汽车均有效。在这两种情况下，被堵塞的汽车都可能忽略并撞到障碍物。而且，诸如掩盖和消声之类的声学安静的方法可以用于超声传感器攻击。

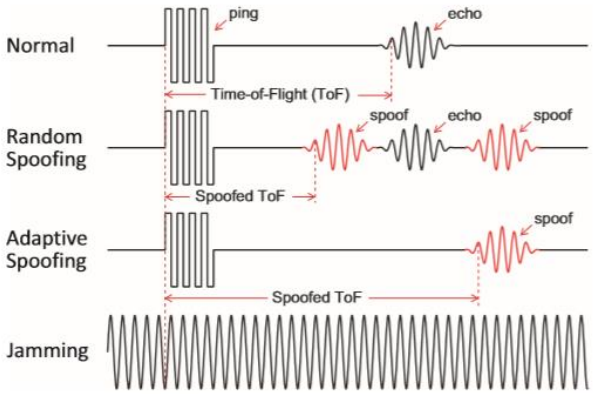

图 8 针对超声波传感器的干扰和注入攻击信号图

在[23]中，提出了两种方法来防御超声传感器的攻击。第一个方法利用了移动波形参数的想法，因此可以验证物理信号。第二种方法使用两个或多个传感器来检测攻击，恢复障碍检测能力或定位攻击者。根据实验，这两种对策可以有效防御超声波传感器的攻击。

摄像头

在自动驾驶汽车中，摄像机用于许多场合，例如交通标志识别，车道检测，障碍物检测等。Petit 等[21]获得了带有多个光源的商业相机系统 MobilEye C2-270 的致盲效率。它表明利用激光或 LED 矩阵足

以使相机蒙蔽。他们还证明了在实验室环境中，攻击者可以不断地打开和关闭照明灯，以使摄像机迷惑。在[22]中，Yan 等通过将 LED 和激光直接对准相机，成功地使相机致盲。特别是，将 LED 灯对准校准板（这是现实场景的替代品）将导致特定区域的隐藏。根据结果，即使在非常短的距离（不到半米）内短短几秒钟内向 AV 摄像机辐射激光束，也会造成不可逆转的损坏，从而破坏相应的自主行为。

由于光学特性导致照相机的脆弱性，因此难以构建完全安全的照相机系统。 尽管如此，Petit 等[21]给出一些可能的对策：冗余，可移动的近红外截止滤光片和光致变色镜片可提供不同方面的适当保护，尽管它们可能有局限性或带来新的问题。

总结

无人驾驶车提供更精确的控制来释放驾驶员的负担的同时也能减少交通事故的发生，从而极大地提高驾驶的便利性。随着人工智能的快速发展和物联网技术的重大进步，我们见证了近年来自动驾驶的稳步发展。尽管前景广阔，但自动驾驶技术的发展也面临着新的挑战，其中安全性是头等大事。本文从传感器的角度对围绕自动驾驶的安全威胁进行了系统的分析。除了对这些威胁的深入概述之外，表 II 总结了本文还归纳的相应防御策略。

表 II：针对传感器的防御策略摘要

防御策略		原则	修改	额外硬件	文献
GPS	信号检测	检查信号固有特性（如强度）	是	视情况	[10]-[16]
	密码学	加密和认证	信号	否	[17]-[19]
激光	冗余	多个激光雷达	否	是	[20]-[21]

雷达	融合	多种传感器	否	是	[20]-[21]
	修改	减小接收角度，多次脉冲激光，缩短脉冲时间间隔	设备	否	[20]-[21]
	随机化	随机旋转或随机脉冲信号	设备/信号	否	[20]-[21]
毫米波雷达	完整性检测	现实世界中不可能使用大功率微波	否	否	[22]
	冗余	多个毫米波雷达	否	是	[22]
	融合	多种传感器融合	否	是	[22]
	随机化	随即脉冲信号	信号	是	[22]
超声波雷达	完整性检测	现实世界中不可能使用大功率微波	否	否	[22]
	冗余	多个超声波雷达	否	是	[22], [23]
	融合	多种传感器融合	否	是	[22]
	随机化	随即脉冲信号	信号	是	[22]
摄像头	冗余	多个摄像头	否	是	[21]
	特殊光学	滤光片和光致变色镜片	设备	是	[21]

参考文献

[1] J. V. Carroll, “Vulnerability assessment of the us transportation infrastructure that relies on the global positioning system,” The Journal of Navigation, vol. 56, no. 2, pp. 185–193, 2003.

[2] J. S. Warner and R. G. Johnston, “A simple demonstration that the global positioning system (gps) is vulnerable to spoofing,” Journal of Security Administration, vol. 25, no. 2, pp. 19–27, 2002.

[3] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O’Hanlon, and P. M. Kintner, “Assessing the spoofing threat: Development of a portable gps civilian spoofer,” in Proc. of Radionavigation laboratory conference proceedings, 2008.

[4] M. L. Psiaki and T. E. Humphreys, “GNSS spoofing and detection,” Proceedings of the IEEE, vol. 104, no. 6, pp. 1258–1270, 2016.

[5] K. C. Zeng, S. Liu, Y. Shu, D. Wang, H. Li, Y. Dou, G. Wang, and Y. Yang, “All your GPS are belong to us: Towards stealthy manipulation of road navigation systems,” in Proc. of 27th {USENIX} Security Symposium ({USENIX} Security), 2018, pp. 1527–1544.

[6] N. O. Tippenhauer, C. Popper, K. B. Rasmussen, and S. Capkun, “On the requirements for successful gps spoofing attacks,” in Proc. of the 18th ACM conference on Computer and communications security
(CCS), 2011, pp. 75–86.

[7] T. Nighswander, B. Ledvina, J. Diamond, R. Brumley, and D. Brumley, “Gps software attacks,” in Proc. of the ACM Conference on Computer and Communications Security (CCS), 2012, pp. 450–461.

[8] A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, “Unmanned aircraft capture and control via gps spoofing,” Journal of Field Robotics, vol. 31, no. 4, pp. 617–636, 2014.

[9] J. Bhatti and T. E. Humphreys, “Hostile control of ships via false gps signals: Demonstration and detection,” NAVIGATION: Journal of the Institute of Navigation, vol. 64, no. 1, pp. 51–66, 2017.
[10] J. S. Warner and R. G. Johnston, “Gps spoofing countermeasures,” Homeland Security Journal, vol. 25, no. 2, pp. 19–27, 2003.
[11] K. D. Wesson, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, “An evaluation of the vestigial signal defense for civil gps anti-spoofing,” in Proc. of Radionavigation Laboratory Conference Proceedings, 2011.
[12] A. Konovaltsev, M. Cuntz, C. Haettich, and M. Meurer, “Autonomous spoofing detection and mitigation in a gnss receiver with an adaptive antenna array,” in Proc. ION GNSS, 2013.
[13] P. Y. Montgomery, T. E. Humphreys, and B. M. Ledvina, “A multiantenna defense: Receiver-autonomous gps spoofing detection,” Inside GNSS, vol. 4, no. 2, pp. 40–46, 2009.
[14] M. L. Psiaki, B. W. O’hanlon, S. P. Powell, J. A. Bhatti, K. D. Wesson, and T. E. Humphreys, “Gnss spoofing detection using two-antenna differential carrier phase,” in Proc. of Radionavigation Laboratory Conference Proceedings, 2014.
[15] S. Daneshmand, A. Jafarnia-Jahromi, A. Broumandan, and G. Lachapelle, “A low-complexity gps anti-spoofing method using a multi-antenna array,” aa, vol. 2, p. 2, 2012.
[16] M. L. Psiaki, S. P. Powell, and B. W. Ohanlon, “Gnss spoofing detection using high-frequency antenna motion and carrier-phase data,” in Proc. of the ION GNSS+ Meeting, 2013, pp. 2949–2991.
[17] B. W. O’Hanlon, M. L. Psiaki, J. A. Bhatti, D. P. Shepard, and T. E. Humphreys, “Real-time gps spoofing detection via correlation of encrypted signals,” Navigation, vol. 60, no. 4, pp. 267–278, 2013.
[18] A. J. Kerns, K. D. Wesson, and T. E. Humphreys, “A blueprint for civil gps navigation message authentication,” in Proc. of IEEE/ION Position, Location and Navigation Symposium (PLANS), 2014, pp. 262–269.
[19] L. Scott, “Anti-spoofing & authenticated signal architectures for civil navigation systems,” in Proc. of the 16th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS/GNSS), 2001, pp. 1543–1552.
[20] H. Shin, D. Kim, Y. Kwon, and Y. Kim, “Illusion and dazzle: Adversarial optical channel exploits against lidars for automotive applications,” in Proc. of International Conference on Cryptographic Hardware and Embedded Systems (CHES). Springer, 2017, pp. 445–467.
[21] J. Petit, B. Stottelaar, M. Feiri, and F. Kargl, “Remote attacks on automated vehicles sensors: Experiments on camera and lidar,” Black Hat Europe, vol. 11, p. 2015, 2015.
[22] C. Yan, W. Xu, and J. Liu, “Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle,” DEF CON, vol. 24, 2016.
[23] W. Xu, C. Yan, W. Jia, X. Ji, and J. Liu, “Analyzing and enhancing the security of ultrasonic sensors for autonomous vehicles,” IEEE Internet of Things Journal, vol. 5, no. 6, pp. 5015–5029, 2018.
[24] S. Brands and D. Chaum, “Distance-bounding protocols,” in Proc. of Workshop on the Theory and Application of of Cryptographic Techniques, 1993, pp. 344–359.
[25] K. B. Rasmussen and S. Capkun, “Realization of rf distance bounding,” in Proc. of the 19th USENIX Security Symposium (USENIX Security), 2010, pp. 389–402.
[26] “Lidar and autonomous technology,” http://velodynelidar.com/newsroom/lidar-

autonomous-technology/, 2016.
[27] A. Francillon, B. Danev, and S. Capkun, “Relay attacks on passive keyless entry and start systems in modern cars,” in Proc. of the Network and Distributed System Security Symposium (NDSS), 2011.
[28] M. Zhou, Q. Wang, K. Ren, D. Koutsonikolas, L. Su, and Y. Chen, “Dolphin: Real-time hidden acoustic signal capture with smartphones,” IEEE Transactions on Mobile Computing, vol. 18, no. 3, pp. 560–573, 2019.
[29] “Lidar vs. radar,” https://www.sensorsmag.com/components/lidar-vsradar, 2018.