ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 8, Issue 5 , May 2021

Review of Techniques for Vulnerability Analysis of Autonomous Cars

Antariksh Pratham, Pramod Sonawane, Sneha Kamble, Siddhi Sali

Student Researcher, Department of Electronics and Telecommunication, Pimpri Chinchwad College of Engineering, Pune
Asst. Professor, Department of Electronics and Telecommunication, Pimpri Chinchwad College of Engineering, Pune
Student, Department of Electronics and Telecommunication, Pimpri Chinchwad College of Engineering, Pune
Student, Department of Electronics and Telecommunication, Pimpri Chinchwad College of Engineering, Pune

ABSTRACT: There has been massive growth in autonomous driving technology in the past few years. This also means that there is a growing need to develop tools and frameworks for us to evaluate the security aspect of such connected technology. The more the number of features we add, we are also increasing the attack surface for a hacker with malicious intent. This is why it is very important to understand the security aspect holistically. Also, we should have some kind of analysis and frameworks that will assist automakers in developing safer and better cars. We have already done a lot of research in this field. In this paper, the authors have reviewed various techniques available for vulnerability analysis of connected and autonomous driving technology in this paper. Different models for autonomous driving and currently adopted methodologies for building such technology are also discussed

KEY WORDS: AWS, GCP, Autonomous Vehicles, Cybersecurity, Cloud Computing, Dev Ops, Dev SecOps

I.INTRODUCTION

With the rapid development of computer vision techniques and of technology in general, autonomous cars are inevitably going to be a reality in the years to come, as early as 2025[1]. Moore's law[2] has enabled us to innovate at an unprecedented speed which made this possible. Autonomous driving technologies will transform transportation as we know it in the years to come[3], [4]. Connected mobility will be an even better-added feature that will allow cars to become even better by communicating among themselves. People have been researching about it for a long time and it looks like now we finally might be seeing autonomous driving, with semi-autonomous and driver-assist features already being in the market right now[5]. People have also experimented with connected cars and the possibilities of having such infrastructure[6], [7]. Companies like Tesla have been advocating autonomous driving for some time now, even saying that they can bring it to consumers soon by using advanced computer vision and onboard processing.[8] Connected and autonomous vehicles have also been demonstrated in North America, Japan, and Europe.[9]–[12]

However, there is a need for us to also understand that as we continue to innovate and redefine the borders of modern-day science, the security aspect of building such sophisticated technology can not be neglected. It is important to know that as we make our cars and essentially other electronics even more connected, we are also allowing hackers to break in with malicious intent[13] and exploit our embedded devices.

That is why there is a growing need for an autonomous vehicle security framework and extensive research should be done on the topic. Many organisations and researchers have made considerable progress in that direction by publishing 0-day exploits and vulnerabilities found in modern-day connected cars[14], [15] and recommending security measures that can be adapted to ensure they are not done again [16].

While there has been considerable research, the automotive community has not been able to develop techniques to defend against the novel attack architectures that are getting developed. That is why it is important to present a comprehensive review of research literature on cyber-attacks that can compromise autonomous vehicles. This can be helpful as companies should be able to understand which methodologies are currently being adopted by the research community and develop effective countermeasures against the same. We have reviewed the various autonomous driving technologies and presented the possible attacks that can be done based upon what others have accomplished.

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 8, Issue 5 , May 2021

II. AUTONOMOUS DRIVING TECHNOLOGY

Autonomous driving technology has been in the market for quite some time now. There have been various attempts at making connected and autonomous cars and deploying them at scale. The United States Department of Transportation carried out the Connected Vehicle Pilot Deployment Program[17], [18], which provided more than $45m to cities like New York City[19], Tampa[20], and Wyoming[21] to develop programs to make such systems a reality in the years to come. The Centre for Connected and Autonomous Vehicles in the UK also invested £120m to support various CAV projects. Chinese officials estimated about 8.6m autonomous vehicles on their roads by as early as 2035. Japanese PM Shinzo Abe wanted to explore using a fleet of autonomous cars for the Tokyo Olympics. Hyundai Motor Corp also organised competitions in South Korea in to stimulate interest and encourage the development of CAVs.

Even though such technologies have become fairly advanced thanks to recent advancements, we should also understand that sometimes it is incredibly dangerous to trust autonomous driving completely. After all, there is a reason the technology is not available to the general public. People have, however, always tried to find loopholes in one way or another and led to fatal crashes and accidents which are being investigated by the NHTSA for various reasons[22]–[24], all related to their complexity and still difficult to understand nature. NHTSA has also gone ahead and done several special investigations also into how driver-assist systems have been the primary cause of such accidents[25] as people gave a little too much faith in these systems.

There are various levels of automation in autonomous cars, which range from no automation to full automation. SAE publishes standards[26], [27] and references for the levels of automation[28]. These five levels of automation are – Level 0 meaning no automation, Level 1 meaning most driver assistance systems, Level 2 meaning partial automation, Level 3 encompassing conditional automation, Level 4 being higher automation, and Level 5 full automation. In this paper, we mostly consider only the higher levels of automation.

An autonomous car, or CAV, contains several components, that enable it to get a better understanding of its environment, like laser, radar, cameras, LiDAR[29], and various connection and networking mechanisms Bluetooth, WiFi, and Wireless Access in Vehicular Environments (WAVE)[30]. These components help the onboard computer get a sense of the environment around it and make calculated decisions to avoid obstacles and travel. We have found applications that utilise various connection protocols for their functioning include, but are not limited to - Intelligent Driver-Assistance Systems (IDAS)[31] and safety features through Vehicle-to-Infrastructure communications [32], and even through Vehicle-to-Vehicle communications [33], [34].

III. AWS DEEPRACER

We are using AWS DeepRacer as the prototype for the purposes of our research. We felt that it is the closest resemblance to an autonomous car due to its structure and basic functioning. The AWS DeepRacer is a $1/18^{th}$ scale race car designed by AWS for enthusiasts to learn the concepts of RL in a fun and engaging way[35]. It consists of an online simulator, a physical car, and a racing league.

We have used the physical car for our prototyping. It has cameras, a gyroscope, accelerometer, and various other sensors making it an autonomous car. The car itself is running on open-source frameworks which makes the development process even easier. The simulator is based on Rviz and Gazebo, which help the car to be trained faster in a cloud-based environment. In terms of AWS services, that translates to AWS RoboMaker and AWS SageMaker. These services along with CloudWatch, Amazon S3 make the basic constituents of the working principle of the car[36].

The car learns in the simulated environment using a combination of RL and PPO methods, which is almost similar to how autonomous cars learn their policy networks in closed testing environments. Using Sim2Real learning[37], the same learning is transferred from the online simulator into the car. This is how the car works.

This paper doesn't cover the AWS DeepRacer in-depth as it is proprietary hardware used by researchers to only prototype and do attacks on.

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 8, Issue 5 , May 2021

IV. POSSIBLE ATTACK METHODOLOGIES

There are various commonly known attacks that can be easily ported and adapted for an embedded environment. With a few changes, you can easily compromise connected cars remotely[38]–[41]. Car manufactures need to have an understanding of the security aspect of these connected and autonomous cars. Even though there haven't been any significant attacks on autonomous cars that caused loss of life, researchers have found very serious loopholes from time to time[42]. The problem with autonomous cars is that in the event of a compromise, there is a good chance the driver is not in a position mentally or physically to take control and initiate immediate corrective action due to the nature of the technology. Researchers have suggested several attacks as well as countermeasures against them highlighting their impact on the infrastructure[38], [43]–[45]. They have identified issues with the sensors, ECUs, and even the network topologies and infrastructure being used, sometimes finding vulnerabilities in production cars as well[46]–[48].

Attack models have been demonstrated on various components such as GPS and LiDAR spoofing[49]–[52], and adversarial attacks on the camera systems[53], [54].

Take the camera for example. Now, the camera is an important aspect of autonomous cars. It helps them with things such as traffic sign recognition[55]–[57] and lane detection[58], [59]. It also provides inputs to Deep Learning models that are deployed in cars to help them drive autonomously. Manufacturers have also tried to replace LiDAR with cameras[8] because it is low cost and we have massive computational algorithms today which can help us cut the high cost of LiDAR. However, cameras can't perform better in tricky situations like rain, fog, or snow[60]. A simple, quick burst of 650 nm laser is enough to blind the camera[61] rendering it almost completely useless and cause irrecoverable damage.

V. EFFECTIVE COUNTERMEASURES

It is also important for us to understand that most of the attacks that we explored can be defended quite easily and without much effort. Thanks to the efforts of researchers in this domain, we know about some of the countermeasures that can be adopted so that cars can be made safer for the average consumers and they are not at risk from hackers and people looking to exploit connected cars.

One of the most effective strategies can be to educate the people about the technology, as well as inform them about advantages and disadvantages. This by far will be the greatest investment any one company can do for it's consumers as they can better understand autonomous driving and understand their responsibility behind using such technology. This will not only defend against attacks but also help in increasing confidence.

Cho. et al (2016) [62]proposed clock-based IDS which measures the clock skew of ECUs and then uses this information to fingerprint the ECUs, thus preventing them for getting tampered with. Intrusions are detected by checking for an abnormal shift in the clock skews. Encryption can also be used where it is currently not implemented, like CAN bus and in signals sent by sensors. Several researchers have published techniques that can be adopted for such signals.[63]–[66] A decentralised public key infrastructure (PKI) can also help secure V2V and V2I communications[67], [68].

VI.CONCLUSION

In this paper, various techniques to evaluate autonomous driving technology have been reviewed. The different tools, frameworks, and methods have been thoroughly reviewed. Also, an overview of different technologies for developing autonomous cars has been discussed. There is a need for us to make technology that is safe in the true sense and holistically. Although a considerable amount of work has been done to make autonomous cars safer,we need to see that these frameworks are properly implemented. That is why we hope this research will be instrumental for car manufacturers and stakeholders in making connected mobility safer by designing and implementing state-of-the-art mitigation and defence strategies.

Safety and security should be the basis of designing for the connected future for everyone to feel trustworthy with their electronics which would have more than surrounded them. It should be important for us to build redundancies and important measures should be taken so that in the event of a compromise, immediate and defensive mechanisms can be

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 8, Issue 5 , May 2021

quickly deployed, thus saving valuable lives. Without it, with the rate at which innovation is progressing, we will only be digging our own hole.

REFERENCES

[1] Z. Kanter, "How Uber's Autonomous Cars Will Destroy 10 Million Jobs and Reshape the Economy by 2025," *Zack's Notes*, 2015. https://zackkanter.com/2015/01/23/how-ubers-autonomous-cars-will-destroy-10-million-jobs-by-2025/

[2] G. E. Moore, "Progress in Digital Integrated Electronics." IEEE, 1975. [Online]. Available: http://ai.eecs.umich.edu/people/conway/VLSI/BackgroundContext/SMErpt/AppB.pdf

[3] and J. M. D. C. L. Figueiredo, I. Jesus, J. T. Machado, J. R. Ferreira, "Towards the development of intelligent transportation systems," in *IEEE Intelligent Transportation Systems (ITSC) (Cat. No. 01TH8585)*, IEEE, 2001, pp. 1206–1211.

[4] J. C. Becker and A. Simon, "Sensor and navigation data fusion for an autonomous vehicle," in *Proceedings of the IEEE Intelligent Vehicles Symposium*, Cat. No. 0., IEEE, 2000, pp. 156–161.

[5] Tesla Motors Inc., "Autopilot and Full Self-Driving Capability." https://www.tesla.com/support/autopilot

[6] P. Bansal and K. M. Kockelman, "Sensor and navigation data fusion for an autonomous vehicle," in *Transportation Research Part A: Policy and Practice*, Vol. 95., 2017, pp. 49–63.

[7] E. Uhlemann, "Autonomous vehicles are connecting...[connected vehicles]," in *IEEE Vehicular Technology Magazine*, Vol. 10., 2015.

[8] S. Ingle and M. Phute, "Tesla Autopilot :Semi Autonomous Driving, an Uptick for Future Autonomy," *International Research Journal of Engineering and Technology*, vol. 3, no. 9, pp. 369–372, 2016, [Online]. Available: www.irjet.net

[9] M. Williams, "Prometheus-the european research programme for optimising the road transport system in europe," in *IEE Colloquium on Driver Information*, 1988.

[10] E. van Nunen, M. R. Kwakkernaat, J. Ploeg, and B. D. Netten, "Cooperative competition for future mobility," in *IEEE Transactions on Intelligent Transportation Systems*, Vol. 13., 2012, pp. 1018–1025.

[11] A. Benmimoun, M. Lowson, A. Marques, G. Giustiniani, and M. Paren, "Demonstration of advanced transport applications in citymobil project," in *Transportation Research Record*, Vol. 2110., 2009, pp. 9–17.

[12] Y. Suzuki, T. Hori, T. Kitazumi, K. Aoki, T. Fukao, and T. Sugimach, "Development of automated platooning system based on heavy duty trucks," *7th IFAC Symposium on Advances in Automotive Control*, 2010.

[13] M. Zoppelt and R. T. Kolagari, "What Today's Serious Cyber Attacks on Cars Tell Us: Consequences for Automotive Security and Dependability," in *Model-Based Safety and Assessment*, SpringerLink, 2019, pp. 270–285.

[14] S. Nie, L. Liu, Y. Du, and W. Zhang, "Over-the-Air : How We Remotely Compromised the Gateway , Bcm , and Autopilot Ecus of Tesla Cars," *Black Hat USA*, vol. 1, pp. 1–19, 2018, [Online]. Available: https://i.blackhat.com/us-18/Thu-August-9/us-18-Liu-Over-The-Air-How-We-Remotely-Compromised-The-Gateway-Bcm-And-Autopilot-Ecus-Of-Tesla-Cars-wp.pdf

[15] S. Nie, L. Liu, and Y. Du, "Free-fall: hacking tesla from wireless to can bus," *Defcon*, pp. 1–16, 2017, [Online]. Available: https://paper.seebug.org/papers/Security Conf/Blackhat/2017_us/us-17-Nie-Free-Fall-Hacking-Tesla-From-Wireless-To-CAN-Bus.pdf%0Ahttps://www.blackhat.com/docs/us-17/thursday/us-17-Nie-Free-Fall-Hacking-Tesla-From-Wireless-To-CAN-Bus-wp.pdf

[16] Z. Cai, A. Wang, W. Zhang, M. Gruffke, and H. Schweppe, "0-days & Mitigations: Roadways to Exploit and Secure Connected BMW Cars," *Black Hat USA*, vol. 2019, p. 39, 2019.

[17] S. Z. D. Gopalakrishna, V. Garcia, A. Ragan, T. English and E. H. R. Young, M. Ahmed, F. Kitchener, N. U. Serulle, "Connected vehicle pilot deployment program phase 1, concept of operations (ConOps), ICF/Wyoming," 2015.

[18] A. R. F. Kitchener, T. English, D. Gopalakrishna, V. Garcia and N. U. S. R. Young, M. Ahmed, D. Stephens, "Connected vehicle pilot deployment program phase 2, data management plan wyoming," 2017.

[19] New York City Department. of Transportation, "NYC Connected Vehicle Project For Safer Transportation." https://cvp.nyc/

[20] Tampa Hillsburg Expressway Authority, "THEA Connected Vehicle Pilot", [Online]. Available: https://www.tampacvpilot.com/

[21] Wyoming Department of Transportation, "Wyoming DOT Connected Vehicle Pilot." https://wydotcvp.wyoroad.info/

[22] K. Habib, J. Quandt, and S. Ridella, "DP 19-005: Battery Management Software Updates," 2019.

[23] K. Habib, J. Quandt, and S. Ridella, "PE 16-007: Automatic vehicle control systems," 2017.

[24] A. Alkondon, S. Ridella, and J. Quandt, "PE 20-010: Loss of rear view camera display," 2020.

[25] Crash Research & Analysis Inc., "Special Crash Investigations: On-Site Automated Driver Assistance System Crash Investigation of the 2015 Tesla Model S 70D," Washington DC, 2018.

[26] B. Sheehan, F. Murphy, M. Mullins, and C. Ryan, "Connected and autonomous vehicles: A cyber-risk classification framework," *Transportation Research Part A: Policy and Practice*, vol. 124, no. xxxx, pp. 523–536, 2019, doi: 10.1016/j.tra.2018.06.033.

[27] J. Shuttleworth, "Levels of Driving," 2018. [Online]. Available: https://www.sae.org/news/2019/01/sae-updates-j3016-automated-driving-graphic

[28] SAE International, "Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles," 2018. https://www.sae.org/standards/content/j3016_201806/

[29] A. A. M. Wyglinski, X. Huang, T. Padir, L. Lai, T. R. Eisenbarth and K. Venkatasubramanian, "Security of autonomous systems employing embedded computing and sensors," *IEEE micro*, vol. 33, pp. 80–86, 2013.

[30] IEEE Standards Association, "IEEE Standard for Information Technology-Local and Metropolitan Area Networks-Specific Requirements-part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments," *IEEE Std 802.11-2016 (Revision of IEEE Std 802.11-2012)*, 2010.

[31] M. Philipovic, D. Spasojevic, I. Velikic, and N. Teslic, "Toward Intelligent Driver-Assist Technologies and Piloted Driving : Overview , Motivation and Challenges," *X International Symposium on Industrial Electronics INDEL 2014*, pp. 10–14, 2014.

[32] A. Böhm and M. Jonsson, "Supporting real-time data traffic in safety-critical vehicle-to- infrastructure communication," *Proceedings - Conference on Local Computer Networks, LCN*, pp. 614–621, 2008, doi: 10.1109/LCN.2008.4664253.

[33] S. Biswas, R. Tatchikou, and F. Dion, "Vehicle-to-vehicle wireless communication protocols for enhancing highway traffic safety," in *IEEE communications magazine*, Vol. 44., 2006, pp. 74–82.

[34] and R. S. Q. Xu, T. Mak, J. Ko, "Vehicle-to-vehicle safety messaging in DSRC," in *1st ACM international workshop on Vehicular ad hoc networks*, ACM, 2004, pp. 19–28.

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 8, Issue 5 , May 2021

[35] AWS, "AWS DeepRacer: Developers, start your engines." https://aws.amazon.com/deepracer/ (accessed Feb. 17, 2021).
[36] AWS, *AWS DeepRacer Documentation*. 2019.
[37] B. Balaji *et al.*, "DeepRacer : Educational Autonomous Racing Platform for Experimentation with Sim2Real Reinforcement Learning".
[38] J. Petit, B. Stottelaar, M. Feiri, and F. Kargl, "Remote attacks on automated vehicles sensors: Experiments on camera and lidar," in *Black Hat Europe*, Vol. 11., 2015.
[39] S. Narain, A. Ranganathan, and G. Noubi, "Security of GPS/INS based on-road location tracking systems," in *IEEE Symposium on Security and Privacy (SP)*, IEEE, 2019, pp. 587–601.
[40] Q. Meng, L. T. Hsu, B. Xu, X. Luo, and A. El-Mowaf, "A GPS Spoofing Generator Using an Open Sourced Vector Tracking-Based Receiver," in *Sensors*, Vol. 19., 2019, p. 3993.
[41] A. Pathre, "Identification of malicious vehicle in VANET environment from DDoS attack," in *Journal of Global Research in Computer Science*, Vol. 4., 2013, pp. 30–34.
[42] J. Petit and S. E. Shladover, "Potential Cyberattacks on Automated Vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 2, pp. 546–556, 2015, doi: 10.1109/TITS.2014.2342271.
[43] N. I. A. Yadav, G. Bose, R. Bhange, K. Kapoor, "Security, vulnerability and protection of vehicular on-board diagnostics," in *International Journal of Security and Its Applications*, 2015, pp. 405–422.
[44] S. C. K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno and H. S. D. McCoy, B. Kantor, D. Anderson, "Experimental security analysis of a modern automobile," in *IEEE Symposium on Security and Privacy*, IEEE, 2010, pp. 447–462.
[45] H. S. S. Checkoway, D. McCoy, B. Kantor, D. Anderson and T. K. S. Savage, K. Koscher, A. Czeskis, F. Roesner, *Comprehensive experimental analyses of automotive attack surfaces," in USENIX Security Symposium*, Vol. 4. San Francisco, 2011.
[46] Y. Cao *et al.*, "Adversarial sensor attack on LiDAR-based perception in autonomous driving," *Proceedings of the ACM Conference on Computer and Communications Security*, pp. 2267–2281, 2019, doi: 10.1145/3319535.3339815.
[47] C. Yan, W. Xu, and J. Liu, "Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle," 2016.
[48] Regulus Cyber LTD, "Tesla model 3 spoofed off the highway – regulus navigation system hack causes car to turn on its own." https://www.regulus.com/blog/tesla-model-3-spoofed-off-the-highway-regulus-researches-hack-navigation-system-causing-car-to-steer-off-road (accessed Jul. 11, 2020).
[49] Y. Y. and J. Xu, "GNSS receiver autonomous integrity monitoring (RAIM) algorithm based on robust estimation," in *Geodesy and geodynamics*, 2016, pp. 117–123.
[50] 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," in *Navigation*, Vol. 60., 2013, pp. 267–278.
[51] Q. Wang, Y. Zhang, Y. Xu, L. Hao, Z. Zhang, T. Qiao, and Y. Zhao, "Pseudorandom modulation quantum secured lidar," in *Optik*, vol. Vol. 126, 2015, pp. 3344–3348.
[52] M. Nouri, M. Mivehchy, and M. F. Sabahi "Target recognition based on phase noise of received laser signal in lidar jammer," in *Chinese Optics Letters*, 2017, pp. 100–102.
[53] C. Sitawarin, A. N. Bhagoji, A. Mosenia, M. Chiang, and P. Mittal, "DARTS: Deceiving Autonomous Cars with Toxic Signs," arXiv:1802.06430.
[54] Y. Man, M. Li, and R. Gerdes, "Poster: Perceived Adversarial Examples," 2019.
[55] J. Levinson, J. Askeland, J. Dolson, and S. Thrun, "Traffic light mapping, localization, and state detection for autonomous vehicles," in *IEEE International Conference on Robotics and Automation*, IEEE, 2011, pp. 5784–5791.
[56] M. O. and S. Omachi, "Traffic light detection with color and edge information," in *2nd IEEE International Conference on Computer Science and Information Technology*, IEEE, 2009, pp. 284–287.
[57] N. F. and C. Urmson, "Traffic light mapping and detection," in *IEEE International Conference on Robotics and Automation*, IEEE, 2011, pp. 521–5426.
[58] A. B. Hillel, R. Lerner, D. Levi, and G. Raz, "Recent progress in road and lane detection: a survey," in *Machine vision and applications*, VOL. 2., 2014, pp. 727–745.
[59] T. Sun, S. Tang, J. Wang, and W. Zhang, "A robust lane detection method for autonomous car-like robot," in *Fourth International Conference on Intelligent Control and Information Processing (ICICIP)*, IEEE, 2013, pp. 373–378.
[60] Y. Wang, W.-L. Chao, D. Garg, B. Hariharan, M. Campbell and K. Q. Weinberger, "Pseudo-lidar from visual depth estimation: Bridging the gap in 3d object detection for autonomous driving," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 2019, pp. 8445–8453.
[61] M. Pham and K. Xiong, "A Survey on Security Attacks and Defense Techniques for Connected and Autonomous Vehicles," pp. 1–24, 2020, [Online]. Available: http://arxiv.org/abs/2007.08041
[62] K. T. C. and K. G. Shin, "Fingerprinting electronic control units for vehicle intrusion detection," in *25th USENIX Security Symposium*, 2016, pp. 911–927.
[63] A. van Herrewege, D. Singelee, and I. Verbauwhede, "CANAuth- a simple, backward compatible broadcast authentication protocol for CAN bus," in *ECRYPT Workshop on Lightweight Cryptograph*, 2011.
[64] J. Halabi and H. Artail, "A lightweight synchronous cryptographic hash chain solution to securing the vehicle can bus," in *IEEE International Multidisciplinary Conference on Engineering Technology (IMCET)*, IEEE, 2018, pp. 1–6.
[65] D. K. Nilsson, L. Sun, and T. Nakajima, "A framework for selfverification of firmware updates over the air in vehicle ECUs," in *EEE Globecom Workshops*, IEEE, 2008, pp. 1–5.
[66] C. W. L. and A. Sangiovanni-Vincentelli, "Cyber-security for the controller area network (can) communication protocol," in *International Conference on Cyber Security*, IEEE, 2012, pp. 1–7.
[67] R. W. van der Heijden, S. Dietzel, T. Leinmuller, and F. Kargl, "Survey on misbehavior detection in cooperative intelligent transportation systems," in *IEEE Communications Surveys & Tutorials*, Vol. 21., IEEE, 2018, pp. 779–811.
[68] "Cyber security of connected autonomous vehicles trialled," *University of Warwick*. https://techxplore.com/news/2019-09-cyber-autonomous-vehicles-trialled.html (accessed Jul. 11, 2020).