World Academy of Science, Engineering and Technology
International Journal of Mechanical and Mechatronics Engineering
Vol:16, No:12, 2022

Artificial Intelligence in Penetration Testing of a Connected and Autonomous Vehicle Network

Phillip Garrad, Saritha Unnikrishnan

***Abstract*—**The increase in connected and autonomous vehicles (CAV) creates more opportunities for cyber-attacks. Cyber-attacks can be performed with malicious intent or for research and testing purposes. As connected vehicles approach full autonomy, the possible impact of these cyber-attacks also grows. This review analyses the challenges faced in CAV cybersecurity testing. This includes access and cost of the representative test setup and lack of experts in the field A review of potential solutions to overcome these challenges is presented. Studies have demonstrated Artificial Intelligence (AI) as a promising technique to reduce runtime, enhance effectiveness and comprehensively cover all the standard test aspects in penetration testing in other industries. However, this review has identified a significant gap in the systematic implementation of AI for penetration testing in the CAV cybersecurity domain. The expectation from this review is to investigate potential AI algorithms, which can demonstrate similar improvements in runtime and efficiency for a CAV model. If proven to be an effective means of penetration test for CAV, this methodology may be used on a full CAV test network.

***Keywords*—**Cybersecurity, connected vehicles, software simulation, artificial intelligence, penetration testing.

I. Introduction

CONNECTED vehicles are a great benefit to the safety on our roads, but can equally also be a threat if not developed safely. The increase of connected vehicles on the road correlates with an increase in the risk of cyber-attacks [1]. This research will review a variety of approaches used to try and mitigate the risk of cyber-attacks on connected vehicles. This review will focus on the design against vulnerabilities during the development phase of a vehicle, increased penetration testing post development, and further testing by academic researchers, or white coat hackers, after release. CAV provide passengers with additional safety, improved operation whilst reducing environment impact. Connected features include over the air traffic updates, emergency breaking alerts, forward collision warning, over the air software updates among other features. These features add safety and help reduce traffic collisions whilst also improving convenience [2].

Cybersecurity is a large element of CAV as with improper protection and safeguarding CAV can be exploited by cybercriminals, causing a risk to public safety, or death [3], [4]. Cybersecurity is considered during vehicle design at a component and a system level. This is then tested at a component level before doing full system testing. Penetration testing, or ethical hacking, is when a simulated cyberattack is performed on a vehicle in a controlled environment. The reason for this testing is to catch and report any vulnerabilities and fix them before cyber criminals find and exploit them. There is a challenge here to catch all vulnerabilities before releasing a product, due to a lack of available talent in penetration testing. It is also difficult to ensure full coverage in penetration testing as their maybe new methods cybercriminals use [5]. There have been a few publications [6], [7] which detail simulated attacks using hardware testbeds and/or software simulated networks. The test approach used and the simulated environment are discussed and detailed in later sections. Initially a deeper dive into general cybersecurity and cyber-attacks will be done. This leads into a review of defense strategies, ethical hacking and lastly how in recent years AI has become an advantage in ethical hacking. Following this a review of cybersecurity in CAV is detailed, leveraging a previously published literature reviews [6] as a foundation. Lastly a look at leveraging similar AI methods utilized in other cybersecurity protocols will be examined for CAV penetration testing before drawing conclusions from the literature review.

II. Cybersecurity

Cybersecurity is a continuously growing field as we a society continue to advance in the Information and Communications Technology (ICT) industry. With the Internet of Things making connections devices and systems there has previously been none, there is a greater need of cybersecurity techniques to safeguard our systems from any kind of information disclosure. Cybersecurity should be a consideration when developing any computer or network related product. Cybersecurity typically presents the picture of needing a hacker with a neon green screen exploiting a network vulnerability to gain access to the user login credentials. Cybercriminals may also attempt to gain such information by social engineering or by phone scams posing as a trusted organization. These types of attacks to gain sensitive information are also a consideration for cybersecurity.

Over the years there has been a wide variety of methods used to enhance cybersecurity of computers and networks, or defense strategies. Table I represents a few of these defense strategies however there is many more mechanisms available [7]. In time, the best practices around these defense strategies can change as cybercriminals learn and develop their attack approach. For

P. Garrad is with faculty of Engineering & Design, Atlantic Technological University Sligo, Ireland (corresponding author, e-mail: phillgarrad@gmail.com).

Dr. S. Unnikrishnan is a lecturer in Computing with the faculty of Engineering & Design, Atlantic Technological University Sligo, Ireland and Principal Investigator with MISHE, Ireland (corresponding author, e-mail: Saritha.Unnikrishnan@atu.ie).

This research was financially supported by the Centre for Mathematical Modelling and Intelligent Systems for Health and Environment (MISHE).

example, to for user login on most systems only a single password was used for user authentication. To improve these multiple defenses, advise was given in a review publication [8]. Now to improve security, two factor authentication is becoming more mainstream.

TABLE I
DEFENSE STRATEGIES

Defense Strategy	Description	References
Fuzzing	Allows detection of software safety errors	[9]
Encryption	Process of encoding information, converting original plaintext into a ciphertext with authorized bodies reverting the cipher.	[10]
Obfuscation	Obfuscation is used to obscure the meaning of the message by making it difficult to understand.	[11]
Anti-Malware	These systems monitor and scan for malware software and remove it.	[12]
Firewall	Monitoring incoming and outgoing network traffic and based on some rules acting on untrusted traffic.	[13]
Access Control	This involves user authentication and 2-factor authentication.	[14]

A. Cybersecurity in CAV

CAV are becoming more connected in recent years there has proportionate increase in the number of cyber-attacks committed against vehicles [1]. To counter this there have been several improvements made to cyber security for CAV. A few are listed in Table II.

TABLE II
CYBERSECURITY IMPROVEMENTS IN RECENT YEARS

Key Terms	Description	References
Fuzzing tools	Fuzz testing is an automated software testing technique which enables testing of various boundary test cases.	[15]
Lattice Model	Lattice Model network for V2X communication which relies on continuous feedback to suppress cyber attacks.	[16]
Anomaly Detection	Use of anti-virus scanners to detect when a cyber-attack has occurred and flag or disconnect from source of attack.	[17]

Each of these approaches have several strengths and weaknesses. The Anomaly detecting is more of repair method as it typically takes an action after the attack has already started. In some cases, the damage has already been done and repairing the attack point will have little benefit to the vehicle. The Fuzzing tools have been proven on a several projects to work effectively however there is the risk that data may be lost or corrupted. The lattice model leverages redundancy to over communicate, that have proven to typically be an effective way to develop automotive systems however it can cost more power and result in some noise.

B. Current Vulnerabilities

In recent years there have been several vulnerabilities found and exploited in CAV by both cyber criminals and white coat hackers. Some of these have since been addressed by Automotive manufacturers. These vulnerabilities are primarily focused on network related weaknesses as these are more relevant to this research. The National Vulnerability Database maintained by the National Institute of Standards and Technology is an excellent source of vulnerabilities. A summary table is shown in Fig. 1 focusing on the five largest auto manufacturers [18] by revenue. Tesla is included in the table due to its world-renowned connectivity and public interest.

TABLE III
VULNERABILITIES FROM THE NIST'S NVD [19]

Automaker	Vulnerability type	Count
Volkswagen		2
	Root level access to infotainment (CVE-2020-28656)	1
	Inject CAN messages (CVE-2018-1170)	1
Toyota		4
	Denial of Service (CVE-2020-5610)	1
	Non Critical access (CVE-2020-5551, CVE-2019-14951, CVE-2018-16546, CVE-2018-1002200)	4
	Man In the middle spoof (CVE-2014-7128)	1
	Command Injection (CVE-2017-1000487)	1
Daimler		8
	Out of Bounds Array Access (CVE-2021-23910)	1
	Remote code execution (CVE-2021-23909, CVE-2021-23908, CVE-2021-23907, CVE-2021-23906)	1
	Eavesdropping (CVE-2019-19563, CVE-2019-19562, CVE-2019-19561, CVE-2019-19560, CVE-2019-19557, CVE-2019-19556)	1
	Eavesdropping (CVE-2018-18071)	1
	Inconvenience (CVE-2018-18070, CVE-2020-16142)	2
	Remote Access (CVE-2009-1283, CVE-2009-1282)	2
General Motors		3
	Information access (CVE-2017-9663)	1
	Man In the middle attack (CVE-2017-12697)	1
	Improper Authentication (CVE-2017-12695)	1
Tesla		15
	Information Access (CVE-2020-9306)	1
	Unauthenticated Vehicle Access (CVE-2020-29440, CVE-2020-29439, CVE-2020-15912, CVE-2018-16806)	4
	Updates accepted without Authentication (CVE-2020-29438)	1
	Denial of Service (CVE-2020-10558, CVE-2019-13582, CVE-2019-13581, CVE-2017-6261, CVE-2009-3277)	5
	Attacker Code execution (CVE-2019-9977)	1
	Command Injection (CVE-2016-9337)	1
	Improper privileges access (CVE-2016-7389, CVE-2016-7382)	2

Table III gives an insight as to what vulnerabilities are out in the world and what is being caught. What is accessible in the NVD gives a general overview on each issue and some links to where it is being tracked. Some of these vulnerabilities are under dispute or have since been fixed however some common trends can be seen. As shown in Table III there is a trend to more vulnerabilities being found and reported in recent years. The large increase in the number of vulnerabilities in 2018-2021 when compared 2009-2017 shows that there is an increase in the number of vulnerabilities detected even if they previously existed and were undetected. As most of the vulnerabilities listed in Table III are related to new features, connected phones, over the air updates, remote key fob control etc., a correlation between new connected features and an increase in

vulnerabilities is demonstrated.

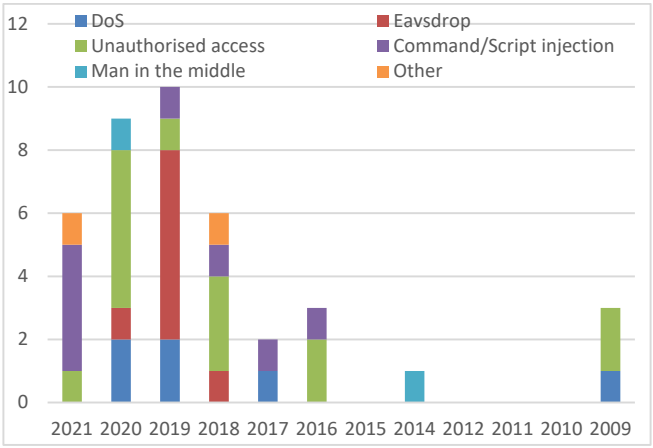

Fig. 1 Security vulnerabilities trends in Top five Automakers

The vulnerabilities listed in the NVD are documented and recorded by MITRE and other similar organizations. This means that the cyber vulnerabilities are found when the product is already released to the public. This highlights the need for more extensive testing by the automaker pre-market.

C. Regulations

In order to protect organizations and to follow best practices there are regulations set out by International Organization for Standardization (ISO) to maintain a high-level safety. One key element of the ISO guidelines for computer security covered under ISO15408 is that cybersecurity must be considered in the full organizational process [20]. There are ISO and Society of Automotive Engineers (SAE) regulatory documents that focus directly on cybersecurity in vehicles including ISO/SAE 21434, Road vehicles - Cybersecurity engineering [21] and SAE Guidelines, SAE J3061 [22]. This regulatory information must be met and the product certified in order for an automotive product to be released. ISO 21434 detailing the regulatory cybersecurity information for automotive was only released in 2021, meaning before that there was only the guidelines being used for handling cybersecurity in automotive. ISO26262 only focuses on functional safety of a vehicle and does not detail cybersecurity regulations. That means vehicles released before the ISO 21434 were developed with significantly less regulation for cyber security. The introduction of ISO 21434 has paved the way to improve vehicle security moving forward by ensuring new technologies in the automotive industry meets the standard set out by this regulation [23].

D. Penetration Testing (Ethical Hacking)

Penetration testing, also known as ethical hacking, has been around since the late nineties. Automotive penetration testing is a controlled attack on automotive software to find any vulnerabilities and access potential damage that can be caused by an attack [24].

There are a few steps to performing a penetration test [25].

1. First the hacker must find an entry point. There are several ways to achieve this; the hacker may have login credentials, the hacker can use a brute force attack, the hacker can pretend to be from a trusted IP, among other methods.
2. Once the hacker has infiltrated the device or network, they can start the penetration test. At this point the hacker can start to target other connected segments of the device or network. A hacker could perform an eavesdropping attack to gain privileged data.
3. Exploit – the hacker builds on the knowledge they have gained and can either disconnect and complete the hack or they can use their findings to exploit the network further. If they have gained elevated privilege, they can now access more data for example.
4. Performing an advanced persistent threat is the ability to access a device or network, maintain it and have the ability to move around while gaining valuable data without being detected. This is the most valuable attack of them all [25]
5. The last step is exfiltration, or to “vanish without a trace”. This involves disconnecting while masking or removing and trace of being there.

Execution of the 5 steps describes a very successful penetration test, however being able to find a vulnerability as in step 1 can be difficult enough. There are many software tools to help with this, including Kali Linux, nmap, burp suite, Nessus and Wireshark.

In Automotive, penetration testing can be done by the automaker or by an outside team that specializes in penetration testing [24]. Using an outside team can be beneficial as they will have limited or no knowledge of the product and so have a same access as a cybercriminal.

E. Artificial Intelligence (AI)

Traditional Penetration testing methods are becoming less favorable in recent years with the advancement of devices due to resource consumption and the variance between systems and so AI has started to be considered as an alternative method [26].

A systematic literature review and meta-analysis of AI in penetration testing completed in 2019 gives an overview on some common AI models used [27]. This details the unique variables and AI models used in the 31 papers analyzed in this literature review. In total there were 10 different independent variables: problem size, number of hosts in exposure, genetic generation, training epoch, network state, number of objectives, action model, AI engine, connectivity, and vulnerabilities. Similarly, there are 10 different AI models used across these papers. It was noted for the most part many models had common approaches, to encompass some degree of attack planning via attack graph generation or attack tree modelling or another form. Based on the attack plan approach the AI model to be used could then be determined. Markov Decision Process (MDP) to some level was used for attack graph generation approaches. Partially Observed MDP was a popular choice here as 9 of the papers used it. Second in use, with 4 papers leveraging it, was the fast-forward model with some using contingent fast-forward model to enhance the results. The meta-analysis concluded this was the highest performing group of models for generating attack plans. Other less used techniques

were multiple value, NuSMV (Model Checker), genetic evolution, reinforcement learning. Some papers used a variety of models. Since this systematic literature review [27] was published in 2019 there has been further papers published supporting the use of reinforcement learning. One states that the use of reinforcement learning is more time efficient, provides reliable outputs, accurate, and covers attack vectors better [26]. In 2020, Hu et al. [28] suggest using Deep Reinforcement Learning for penetration testing. This deep reinforcement learning technique leverages the Deep Q-Learning Network (DQN). Using an attack tree methodology, a reward system is constructed and used to train the DQN. This case achieved an accuracy rate of 86% for selection the correct attack route from the attack plan.

Focusing just on AI in automotive cybersecurity, AI is not a brand-new concept to automotive cyber security. It is proven to be a useful method in cyber defense. A European project CARAMEL [29] uses advanced AI techniques to detect cyberthreats to the internal and external perception modules. Kyrkou et al. shared little information as to the type of AI model they used, which would have been useful information for the current research. Kamel et al. [30] use AI for advanced misbehavior detections but again does not detail the algorithm used.

Another application of AI and machine learning is automating the process of finding vulnerabilities in a system's network. In some cases, reinforcement learning, a machine learning algorithm that learns through trial and error of its environment, is used as an AI solution for penetration testing in general cybersecurity [31]. The focus of the current research is reusing these techniques for automotive. Mckinnell et al. [6] showed that a wide variety of AI models are available to be used in penetration testing but the challenge is to find the best types to fit the simulation.

F. Reinforcement Learning and Q-Learning

Reinforcement learning is a technique that enables the AI agent to interact with an environment and learn from trial and error of the received result [32]. Hanem et al. [26] state that the use of Reinforcement Learning provides better time efficiency, reliable outputs, accuracy, and covers more attack vectors when used for penetration in general, i.e. not CAV specific. Reinforcement is basically a MDP where the agent performs an action based on the observations and feedback from the environment, which is illustrated in Fig. 2. After each loop the outputs are stored in a learning table. The next time the same observation is made so that the agent can predict the feedback/ reward for a given action. The principle of Reinforcement Learning is all actions are tested for all available observable states and the learning table is updated. Each run of the environment from start to finish is known as an episode.

Q-Learning is a reinforcement learning algorithm that seeks to find the best action to take based on the observed state. The best action refers to the action that will return the highest reward. The learning table, or Q-Table, stores the best action based on the training so far. In each step of each episode the best-known action is selected from the Q-Table or, randomly, a different action is selected. If the random action receives a higher reward the Q-Table will be updated with this new action.

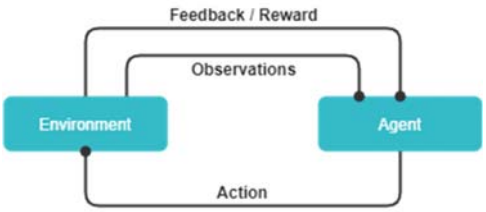

Fig. 2 MDP for Reinforcement Learning [33]

III. CAV Network Testbed Simulation

This section reviews research to find a suitable testbed which can be used for completing this research. Initially both software and hardware solutions were considered however a software would be preferable. From findings an appropriate testbed would then be used for this study.

Initial search results presented promising looking publications such as "Towards a Testbed for Automotive Cybersecurity" by [34]. This referred to a software simulation tool called CANoe, produced by Vector. The paper was however very brief and did not detail how this simulated vehicle model was produced through CANoe or how the hardware was then connected to set it up as a useable testbed. Another paper leverages ROS to create a software and hardware solution [35]. From the title this paper expresses a low cost open-source testbed to enable automated vehicle research however on further reading the product of this paper is merely an interactive way of controlling a real vehicle. It is not a software simulation and requires full access to a vehicle for use and so is not an appropriate solution. From this a leaner search for software simulated solutions was taken.

Some auto manufacturers have also tried to introduce cost effective testbed solutions that do not require access to a vehicle. Toyota produces a Portable Automotive Security Testbed with Adaptability (PASTA) in 2018 [36]. PASTA consists of a hardware representation of a connected vehicle, involving a 4 Embedded Electronic Control Units (ECUs); a Central Gateway (CGW), and the other 3 to control powertrain, body and chassis domains. These are then connected using CAN to inputs. The input control can be doing using a manual input or by using the inbuilt software. From the initial release of PASTA, it looked to be an effective testbed and further papers have backed this up [37], [38]. One drawback of PASTA as mentioned by Baar, and further discovered by some price comparisons online is that the testbed is ~$28,000 which leaves it out of reach for most individual researchers and hence is unsuitable for this current research. Despite PASTA being marketed for research projects, the price of a PASTA system makes it primarily suitable for researchers positioned within large companies. Baar provided a prototyped alternative to PASTA at a much lower budget of approximately €398 which used Raspberry Pi for the ECUs and a CAN bus for streaming data between them [37]. This was certainly a cheaper option, but it sacrificed the amount of data and control that was been

transferred within the vehicle, i.e., it was not setup to take additional inputs such as driver's inputs, nor was the ECU programmed to handle typical vehicle systems, such as powertrain, body or chassis control like PASTA was.

As an appropriate vehicle testbed was not obtainable without further developing a solution, the search parameters were re-evaluated. Instead of viewing messages on an inter vehicular level, viewing the vehicles on a nodular level provided significantly more hits [39], [40]. Simulation tools such as SUMO, OMNeT++, VEINS and INET were used in these cases to build a working simulation of a Vehicular Ad hoc NETwork (VANET). A VANET consists of groups of moving or stationary vehicles connected by a wireless network.

IV. Conclusions

By applying the methodology learnt from this literature review, some of the challenges in the CAV cybersecurity area can be overcome. From reviewing the current literature on AI in cybersecurity and particularly in automotive, it is evident that there is a gap in using AI in automotive cybersecurity. When it comes to testing cybersecurity there is clear benefit set out in industries of leveraging AI models to improve runtime and to establish the best attack plans. From the meta-analysis review, it is clear AI models with an established attack plan had a better chance of success. An attack tree should also be designed to complete the process. Using a MDP partially or fully observable was a common approach taken in other industries and proved to have positive results. Applying a reinforcement learning technique is hard due to the complexity of an automotive environment. However, creating a simulation environment to evaluate some selected scenarios would be the best approach to test the potential of reinforcement learning models in CAV security. This work could be expanded to other areas of CAV if proved beneficial.

Regarding the simulation, the open-source software VEINS is fit for purpose and has been used in similar projects. Implementing and creating open-source versions of simulated cyber-attack scenarios [30] give this project an excellent start point for understanding the simulation environment and the python/C++ bridge allows AI models to be implemented in python and injected into the simulation.

Acknowledgment

This research was financially supported by the Centre for Mathematical Modelling and Intelligent Systems for Health and Environment. The authors wish to thank the Atlantic Technological University of Ireland for the support and guidance in this research. This research was carried out as part of the P. G.'s thesis for a Master in Connected and Autonomous Vehicles course. The authors would like to thank Dr. Donny Hurley for his review and feedback. P. G thanks Sharon George for support and review.

References

[1] K. Kim, J. S. Kim, S. Jeong, J. Park, H. K. Kim, "Cybersecurity for autonomous vehicles: Review of attacks and defense," Computers & Security, vol. 103, no. 102150, p. 27, 2021.

[2] J. Jadaan, S. Zeater, Y. Abukhalil, "Connected Vehicles: An Innovative Transport Technology," in 10th International Scientific Conference Transbaltica 2017: Transportation Science and Technology, Vilnius, 2017.

[3] A. Greenberg, "Hackers Remotely Kill a Jeep on the Highway - With Me in It," Wired, 21 July 2015. (Online). Available: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/. (Accessed 17 06 2021).

[4] F. Lambert, "The Big Tesla Hack: A hacker gained control over the entire fleet, but fortunately he's a good guy," Electrek, 27 08 2020. (Online). Available: https://electrek.co/2020/08/27/tesla-hack-control-over-entire-fleet/. (Accessed 10 06 2021).

[5] D. Tobok, "How Does Penetration Testing Work?," 20 03 2019. (Online). Available: https://cytelligence.com/how-does-penetration-testing-work/. (Accessed 24 10 2021).

[6] D. R. Mickinnel, T. Dargahi, A. Dehghantanha, K. R. Choo, "A systematic literature review and meta-analysis on artificial intelligence in penetration testing and vulnerability assessment," Computers and Electrical Engineering, vol. 75, pp. 175-188, 2019.

[7] M. Lezzi, M. Lazoi, A. Corallo, "Cybersecurity for Industry 4.0 in the current literature: A reference framework," Computers in Industry, vol. 103, pp. 97-110, 2018.

[8] H. Murray, D. Malone, "Costs and benefits of authentication advice.," ArXiv, vol. abs/2008.05836, p. 34, 2020.

[9] M. Sergey, S. Nikolay. E. Sergey, "Cyber security concept for Internet of Everything (IoE)," in 2017 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SINKHROINFO), Kazan, 2017.

[10] R. Sharma, S. Dangi, P. Mishra, "A Comprehensive Review on Encryption based Open Source Cyber Security Tools," in 2021 6th International Conference on Signal Processing, Solan, 2021.

[11] H. Xu, Y. Zhou, J. Ming, M. Lyu, "Layered obfuscation: a taxonomy of software obfuscation techniques for layered security," 03 04 2020. (Online). Available: https://cybersecurity.springeropen.com/articles/10.1186/s42400-020-00049-3. (Accessed 20 11 2021).

[12] A. Hassanzadeh, S. Modi, S.Mulchandani, "Towards effective security control assignment in the Industrial Internet of Things," in 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), Milan, 2015.

[13] C. Sandberg, B. Hunter, "Cyber security primer for legacy process plant operation," in 2017 Petroleum and Chemical Industry Technical Conference (PCIC), Calgary, 2017.

[14] R. Chaturvedi, "UL testing standards to mitigate cybersecurity risk ~ UL's approach with complement to the other standards for SICE 2017," in 2017 56th Annual Conference of the Society of Instrument and Control Engineers of Japan (SICE), Kanazawa, 2017.

[15] X. Ji, H. Cheng, Security Improvements in Connected Cars - Case Study: CEVT Connected Cars, 1st ed., Gothenburg: Chalmers tekniska högskola, 2019.

[16] C. Zhai, W. Wu, "Designing continuous delay feedback control for lattice hydrodynamic model under cyber-attacks and connected vehicle environment," Communications in Nonlinear Science and Numerical Simulation, vol. 95, no. 105667, p. 17, 2020.

[17] G. Rajbahadur, A. Malton, A. Walenstein, A. Hassan, "A Survey of Anomaly Detection for Connected Vehicle Cybersecurity and Safety," Changshu, 2018.

[18] T. Team, "Top 10 Biggest Car Manufacturers by Revenue (2021)," Thread in Motion, 27 07 2021. (Online). Available: https://www.threadinmotion.com/blog/top-10-biggest-car-manufacturers-by-revenue. (Accessed 20 11 2021).

[19] N. I. o. S. a. Technology, "National Vulnerability Database," U.S. Department of Commerce, Gaithersburg, 2021.

[20] G. Burzio, G. F. Cordella, M. Colajanni, M. Marchetti, D. Stabili, "Cybersecurity of Connected Autonomous Vehicles: A ranking based approach," Milan, 2018.

[21] Technical Committee ISO/TC 22/SC 32, "ISO/SAE 21434:2021 Road vehicles — Cybersecurity engineering," 08 2021. (Online). Available: https://www.iso.org/standard/70918.html. (Accessed 20 11 2021).

[22] Issuing Committee: Vehicle Cybersecurity Systems Engineering Committee, "Cybersecurity Guidebook for Cyber-Physical Vehicle Systems J3061_201601," 14 01 2016. (Online). Available: https://www.sae.org/standards/content/j3061_201601/. (Accessed 2021 11 20).

[23] H. Hoeberechts, "How ISO 21434 Will Transform the Automotive

Industry," Mirai, 21 10 2020. (Online). Available: https://www.miraisecurity.com/blog/how-iso-21434-will-transform-the-automotive-industry. (Accessed 20 11 2021).
[24] A. Beliba, A. Kukoba, Vladyslav V., "Automotive Security Testing 101: Requirements, Best Practices, Tips on Overcoming ChallengesIt was originally published on https://www.apriorit.com/," 09 09 2021. (Online). Available: https://www.apriorit.com/dev-blog/742-cybersecurity-automotive-security-testing. (Accessed 21 11 2021).
[25] R. Shimonski, "How to Perform a Penetration Test," in Penetration Testing for Dummies, Wiley, 2020, p. 256.
[26] M. C. Hanem, T. M. Chen, "Reinforcement Learning for Efficient Network Penetration Testing," MDPI - Information 2020, vol. 11, no. 6, p. 23, 2019.
[27] Dean Richard McKinnel, Tooska Dargahi, Ali Dehghantanha, Kim-Kwang Raymond Choo, "A systematic literature review and meta-analysis on artificial intelligence in penetration testing and vulnerability assessment," Computers and Electrical Engineering, vol. 75, pp. 175-188, 2019.
[28] Z. Hu, R. Bueran, Y. Tan, "Automated Penetration Testing Using Deep Reinforcement Learning," in 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Genoa, 2020.
[29] C. Kyrkou, A. Papachristodoulou, T. Theocharides, A. Kloukiniotis, A. Papandreou, A. Lalos, K. Moustakas, "Towards artificial-intelligence-based cybersecurity," in IEEE Computer Society Annual Symposium on VLSI, Limassol, 2020.
[30] J. Kamel, M. R. Ansari, J. Petit, A. Kaiser, I. Jemaa and P. Urien, "Simulation Framework for Misbehavior Detection," IEEE Transactions on Vehicular Technology, vol. 69, no. 6, pp. 6631-3344, 2020.
[31] F. M. Zennaro, L. Erdodi, "Modeling Penetration Testing with reinforcement learning using capture-the-flag challenges and tabular Q-learning," 26 May 2020. (Online). Available: https://arxiv.org/abs/2005.12632. (Accessed 30 September 2021).
[32] R. S. Sutton; A. G. Barto, Reinforcement Learning: An Introduction, Cambridge: MIT Press, 2018.
[33] Y. Feng, "Create a customized gym environment for Star Craft 2," 25 11 2019. (Online). Available: https://towardsdatascience.com/create-a-customized-gym-environment-for-star-craft-2-8558d301131f. (Accessed 17 04 2022).
[34] D. S. Fowler, M. Cheah. S. A. Shaikh, J. Bryans, "Towards A Testbed for Automotive Cybersecurity," Tokyo, 2017.
[35] A. Costley, C. Kunz, R. Gerdes, R. Sharma, "Low Cost, Open-Source Testbed to Enable Full-Sized Automated Vehicle Research," Systems and Control, 2020.
[36] T. Toyama, T. Yoshida, H. Oguma, T. Matsumoto, "PASTA: Portable Automotive Security Testbed with Adaptability," London, 2018.
[37] S. Baar, "Cheap Car Hacking for Everyone A Prototype for Learning about Car Security," Regensburg, 2020.
[38] K. J. Higgins, "Toyota Prepping 'PASTA' for its GitHub Debut," 2019. (Online). Available: https://www.darkreading.com/vulnerabilities-threats/toyota-prepping-pasta-for-its-github-debut. (Accessed 2021 11 14).
[39] D. Jiaa, J. Suna, A. Sharma, Z. Zhenga, B. Liu, "Integrated simulation platform for conventional, connected and automated driving A design from cyber–physical systems perspective," Transportation Research Part C, vol. 124, no. 102984, p. 19, 2021.
[40] F. AAlhaidari, A. Alrehan, "Asimulation work for generating a novel dataset to detect distributed denial of service attacks on Vehicular Adhoc NETwork systems," international Journal of Distributed Sensor Networks, vol. 17, no. 3, p. 25, 2021.