23rd EURO Working Group on Transportation Meeting, EWGT 2020, 16-18September 2020, Paphos, Cyprus

A benchmarking framework for cyber-attacks on autonomous vehicles

A.Khadka[a], P. Karypidis[b], A. Lytos[b], G. Efstathopoulos[a]

[a]0INF, UK
[b]SH, CYPRUS

Abstract

In this paper, a novel framework for a benchmark system for autonomous vehicle focusing of their security reliability is propose. Computer vision and networking technologies are improving offering solutions towards automation in connected autonomous vehicles. These systems are using sensor technologies, including vision and communication, providing information and measurements for the environment and other connected vehicles. As results, unlike conventional vehicles, autonomous vehicles have to communicated with other vehicles as well as other external network infrastructure. However, such requirements make autonomous vulnerable to the attack. This may also motivate various type of cyber threats and attacks like traffic signs modification, GPS spoofing, and Vehicular Adhoc network distributed denial of service. Hence, this paper explores various aspect of security issues, vulnerabilities, exploitation methods and the adverse effect of them on connected autonomous vehicles and propose a novel benchmark framework focusing on physical and communication-based attack to evaluated and assets the state-of-the-art technologies that are currently use during cyber-attack. Connected and Autonomous Vehicles (CAVs) integrate different technologies and communication tools aiming to offer a driver-less, safe, and efficient transportation. Communication between vehicles and infrastructure is an integral part towards the deployment of a CAVs on the real environment, allowing the exchange of data such as position, speed and expected traffic. The connectivity technologies that are used assist on the configuration of the vehicle's behaviors exploiting information gained from sensor and network communication through the observation of the environment. Computer vision and networking technologies provide solutions towards the complete automation in CAVs through the accomplishment of different sub-task. A CAV's computational system is not a centralized one, but it has different components which are responsible for different communication processes due to the need for communication with other vehicles as well as other external network infrastructure. While the communication itself is necessary for autonomous vehicles to operate efficiently, it also increases the problems in aspects of cyber-security. As with all interconnected computing infrastructure, the increase in the number of connected technologies increases the vulnerability of the system in potential cyber (and physical) threats and attacks. The commercial production of CAVs implies an increase in both computing resources and connectivity technologies. The addition of connected hardware and technologies leads to the increase of potential vulnerabilities and therefore creates an unexplored area on the cybersecurity domain. The heterogeneity of the incoming data (digital images, sensor measurements, radio signals, etc.) requires a holistic approach to face the increasing likelihood of future cyber-attacks. Existing benchmark systems in the CAV domain either focus on the performance of the vehicle and its system in Wang et al. (2018), either they are limited to certain parts of the vehicles in Schops et al. (2017) or Benzadan et al. (2019) without considering scenarios for potential cyber-attacks. On the other hand, the research which are focused on encountering cyber-attacks in Kuman et al. (2018) do not propose a complete framework for the evaluation of each system's performance. Therefore, there is a necessity for research in constructing the proper framework for cyber-attacks to CAV.

This paper explores various aspect of security issues, vulnerabilities, exploitative methods, and the adverse effect of them on the connected autonomous vehicles and human passengers or pedestrians. Furthermore, a novel benchmark framework focusing on physical and communication-based cyber-attacks is proposed allowing the evaluation and assessment of the state-of-the-art technologies that are currently used in the CAVs. The proposed framework is designed to face multiple types of attacks, both physical like traffic sign modifications, and cyber such as disruption on the network flow. More specifically, it allows the evaluation of existing solutions of autonomous vehicles supporting attacks based on additive noise, information loss, patterns, and adversarial deep networks for the traffic signs. Regarding the network flow and the communication systems attacks such as PortScan, FTP –BruteForce, Bot, DoS and SSH –Bruteforce are also integrated allowing the evaluation of existing systems under these adverse conditions. The proposed benchmark framework implements a module-based architecture allowing the users to

Peer-review under responsibility of the scientific committee of the 23rd EURO Working Group on Transportation Meeting.

dynamically integrate their modules expanding the potential of this system offering support to other scenarios and sensors. The framework consists of four modules a) Input Interface module (IIM) which handles the input for the framework. The IIM is divided into two further categories, vision-based input and network-based input. Followed by Attack Data Augmentation Module (ADAM) which deals with the attack data simulation and generation process. The module augment both vision and network-based attacks. Thereafter, Detection modules (DM) detects the attacks. The module applies both traditional machine learning approaches as well as deep learning approach to detect the attack. Finally, the evaluation module defines the metrics used for the evaluation purpose.

Peer-review under responsibility of the scientific committee of the 23rd EURO Working Group on Transportation Meeting.
Keywords: benchmarking framework; cyber-attack; autonomous vehicle

References

Behzadan, V., Munir, A., 2019. Adversarial reinforcement learning framework for benchmarking collision avoidance mechanisms in autonomous vehicles. IEEE Intelligent Transportation Systems Magazine.

Kumar, A.D., Chebrolu, K.N.R., KP, S., 2018. A brief survey on autonomous vehicle possible attacks, exploits and vulnerabilities. arXiv preprint arXiv:1810.04144.

Schops, T., Schonberger, J.L., Galliani, S., Sattler, T., Schindler, K., Pollefeys, M., Geiger, A., 2017. A multi-view stereo benchmark with high-resolution images and multi-camera videos, in: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. pp. 3260–3269.

Wang, Y., Liu, S., Wu, X., Shi, W., 2018. CAVBench: A Benchmark Suite for Connected and Autonomous Vehicles, in: 2018 IEEE/ACM Symposium on Edge Computing (SEC). Presented at the 2018 IEEE/ACM Symposium on Edge Computing (SEC), pp. 30–42. https://doi.org/10.1109/SEC.2018.00010