World Academy of Science, Engineering and Technology
International Journal of Transport and Vehicle Engineering
Vol:16, No:05, 2022

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

Authors : Phillip Garrad, Saritha Unnikrishnan

Abstract : The recent popularity of connected and autonomous vehicles (CAV) corresponds with an increase in the risk of cyber-attacks. These cyber-attacks have been instigated by both researchers or white-coat hackers and cyber-criminals. As Connected Vehicles move towards full autonomy, the impact of these cyber-attacks also grows. The current research details challenges faced in cybersecurity testing of CAV, including access and cost of the representative test setup. Other challenges faced are lack of experts in the field. Possible solutions to how these challenges can be overcome are reviewed and discussed. From these findings, a software simulated CAV network is established as a cost-effective representative testbed. Penetration tests are then performed on this simulation, demonstrating a cyber-attack in CAV. Studies have shown Artificial Intelligence (AI) to improve runtime, increase efficiency and comprehensively cover all the typical test aspects in penetration testing in other industries. There is an attempt to introduce similar AI models to the software simulation. The expectation from this implementation is to see similar improvements in runtime and efficiency for the 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
Conference Title : ICACV 2022 : International Conference on Automotive and Connected Vehicles
Conference Location : Montreal, Canada
Conference Dates : May 23-24, 2022