A Simulation-Based Framework for Connected Vehicle Cybersecurity Impact Assessment

Don Nalin Dharshana Jayaratne[1], Suraj Harsha Kamtam[2], Qian Lu[3], Rakib Abdur[4], Muhamad Azfar Ramli[5], Rakhi Manohar Mepparambath[6], Siraj Ahmed Shaikh[7], Hoang Nga Nguyen[8]

Abstract

As connected vehicle technologies become increasingly prevalent, offering groundbreaking capabilities for vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications, the promise for improved traffic safety, efficiency, and sustainability has never been higher. However, this new frontier of transportation also brings unprecedented cybersecurity challenges that can compromise not just individual vehicles but entire traffic ecosystems. Vulnerabilities in these systems have the potential to cascade through transport networks, causing disruptions that extend beyond the initially affected vehicles to impact public safety, traffic flow, and operational efficiency. Incidents like the 2015 Jeep Cherokee hack by Miller and Valasek and the 2022 cyberattack on Russia's Yandex Taxi service demonstrate the severity of these challenges. In both cases, individual vulnerabilities escalated to disrupt broader systems—whether that meant remote control over a single vehicle's functions or sending hundreds of taxis to a single location, paralyzing a city's transportation grid. The ISO/SAE 21434 standard for Road Vehicles — Cybersecurity Engineering has emerged as a critical guideline in response to the growing threats posed by cyber vulnerabilities in the automotive sector. ISO/SAE 21434 focuses primarily on the in-vehicle system and delineates the structure of cybersecurity processes, providing detailed guidance on risk mitigation. However, this current framework has limitations. For instance, its risk assessment clause mainly addresses components within or on the vehicle's perimeter and is not designed to consider the systemic impact on broader transport networks. Additionally, the risk quantification based on the standard predominantly relies on assessor expertise, posing challenges for evaluating risks at the complex, interconnected transport systems level. To address these gaps, our study introduces a novel simulation-based framework to assess cybersecurity threats' operational impact on intelligent transport systems. While the existing ISO/SAE 21434 standard serves as a vital starting point, it falls short of capturing the cascading effects of cyber threats across an entire transportation network. Our framework aims to overcome this limitation by simulating realistic attack scenarios and their ripple effects throughout a transport system, capturing the immediate and cumulative operational impacts. The framework would offer insights to transport planners and automotive cybersecurity analysts, allowing for the development of more effective mitigation strategies. Our proposed simulation-based framework is designed to incorporate real-world cyber-attack scenarios from incident reports and academic literature for impact assessment. Currently, our development efforts are concentrated on the traffic layer simulation; however, it is planned to extend the framework to incorporate the network layers to create a robust representation of a connected vehicle ecosystem. The simulation has attacker models that interact with the simulated environment to trigger specific attack scenarios, which in turn gives rise to damage scenarios. We derive incident impact metrics based on the fundamental traffic flow parameters: speed, flow and density, focusing on operational disruptions within the transportation network. These metrics provide an impact assessment that captures the consequences of a cyberattack, offering critical insights into the potential cascading effects on a transport system's operational integrity. In summary, our simulation-based framework provides an innovative approach to assess the operational impact of cybersecurity threats on intelligent transport networks. By integrating real-world attack scenarios, multi-layer simulations, and a tailored attacker model, the framework offers a deeper view of the potential consequences of cyber threats. This enables a more in-depth understanding of vulnerabilities and informs the development of more effective, context-sensitive mitigation strategies. Given the increasing prevalence and complexity of connected vehicle technologies, our framework will be valuable for researchers and industry stakeholders in evaluating the potential consequences of cyber-attacks on intelligent transport systems.

Keywords: *Intelligent Transportation Systems, Automotive cybersecurity, traffic simulation, transport network impact*

Authors Details.

1. Research Intern, A*STAR Research Institute, Singapore. nalin.jayaratne@gmail.com
2. Student, Centre for Future Transport and Cities, Coventry University, United Kingdom, kamtams@uni.coventry.ac.uk
3. Assistant Professor in Connected and Autonomous Vehicles, Centre for Future Transport and Cities, Coventry University, United Kingdom, ad5271@coventry.ac.uk
4. Associate Professor (Systems Security), Centre for Future Transport and Cities, Coventry University, United Kingdom, ad9812@coventry.ac.uk
5. Deputy Dept Director & Principal Scientist, Institute of High Performance Computing, A*STAR, Singapore, ramlimab@ihpc.a-star.edu.sg
6. Senior Scientist, Institute of High Performance Computing, A*STAR, Singapore, rakhimm@ihpc.a-star.edu.sg
7. Professor in Systems Security, Computer Science, Systems Security Group, Department of Computer Science, Swansea University, United Kingdom, s.a.shaikh@swansea.ac.uk
8. Associate Professor in Cyber Security, Computer Science, Systems Security Group, Department of Computer Science, Swansea University, United Kingdom, h.n.nguyen@swansea.ac.uk