Demo: Leveraging BeamNG Simulation Environment for Automotive Security Research

Samuel C. Hollifield
Oak Ridge National Laboratory

Kevin D. Spakes
Oak Ridge National Laboratory

Nathan Sutherland
Oak Ridge National Laboratory

Abstract

Cybersecurity research on vehicle systems is constrained by the cost of physical test vehicles and the proprietary nature of OEM signal definitions. We present a middleware that bridges the BeamNG.Tech vehicle simulation platform and a physical CAN network, translating in-game vehicle sensor state into standards-compliant J1939 CAN messages in real time. The middleware currently extracts 22 signals aligned with the ORNL Driver Identification Dataset and emits them onto a live CAN bus via commodity hardware, enabling controlled replication of real-world driving studies without physical vehicle access. We describe the system architecture, J1939 signal mapping methodology, and a planned validation study against the original dataset. Future work will integrate CAN injection to support safe, repeatable cyberattack simulation. All source code will be released publicly.

1 Introduction

Rigorous vehicle cybersecurity research requires realistic CAN bus data collected under repeatable, controlled conditions. Physical test vehicles are expensive to instrument and operate, and the signal definitions on most production CAN networks are OEM-proprietary, making cross-platform reproduction difficult without direct manufacturer involvement. Existing simulation approaches have largely relied on synthetic CAN traffic generators or hardware-in-the-loop benches [5], neither of which captures the full coupling between vehicle dynamics and bus state present in real driving data. Verma et al. [4] document this scarcity of high-fidelity, labeled CAN datasets as a persistent barrier to automotive IDS research.

We address this gap with a middleware layer that couples **BeamNG.Tech** [1], a physics-based simulation platform with a Python API for runtime vehicle state access, to a physical CAN network via real-time J1939 message generation. Our middleware maps BeamNG.Tech sensor outputs to J1939 Parameter Group Numbers (PGNs) and Suspect Parameter Numbers (SPNs) [2], and emits standards-compliant CAN frames using commodity interface hardware. To our knowledge, no prior work has used a physics-based simulation engine to generate standards-compliant J1939 CAN traffic for cybersecurity research.

To validate the approach, we target the **ORNL Driver Identification (DriverID) Dataset** [3], which captured 22 driving behavior signals from 50 drivers operating a 2014 Kenworth T270 Class 6 commercial truck. By replicating this exact signal set in simulation and comparing resulting distributions against the original data, we characterize the fidelity of simulated CAN traffic as a proxy for real-world collection.

1.1 Middleware Architecture

The middleware runs as a Python process on Windows, polling the BeamNG.Tech API at configurable intervals and executing the following pipeline per sample:

1. **Signal extraction**: The 22 signals from the DriverID feature characterization study, including wheel speed, engine RPM, accelerator pedal position, and brake input, are read from the BeamNG.Tech vehicle state and normalized to the physical units defined by their target J1939 SPNs.
2. **J1939 encoding**: Each signal is encoded into its target PGN frame per the SAE J1939 SPN scaling, offset, and bit-position specifications. Signal-to-SPN mappings are enumerated in Table 1.
3. **CAN transmission**: Encoded frames are transmitted via a **Kvaser Leaf Light v2** USB-CAN interface using the `python-can` library, producing bus traffic format-equivalent to that of a real heavy-duty vehicle ECU.

1.2 Signal Mapping

Mappings were constructed by identifying the J1939 SPN whose physical definition most closely corresponds to each BeamNG.Tech sensor output.

DriverID Signal	PGN	SPN
Engine RPM	61444	190
Vehicle Speed	65256	84
Accelerator Position	61443	91
Wheel Speed (FL/FR/RL/RR)	65215	905-908
Brake Switch	61441	1121
[*remaining signals — to be completed*]		

Table 1: J1939 SPN mappings for DriverID signals (partial).

2 Validation Approach

We validate against the DriverID Dataset [3], which provides ground-truth signal distributions for the 22 features used in driver identification. Simulated drives are executed in BeamNG.Tech along routes approximating the original collection conditions; the resulting J1939 CAN logs are compared against the real dataset via per-signal statistical distribution analysis, focusing on pedal dynamics, speed profiles, and wheel speed differentials. A secondary objective is to evaluate whether models trained on real DriverID data generalize to simulated data and vice versa, assessing simulation as a low-cost augmentation for driving behavior studies.

3 Demonstration

We will demonstrate the complete pipeline live at the poster session. BeamNG.Tech will run on a laptop with the middleware translating vehicle sensor state to J1939 CAN frames in real time. Attendees can drive the simulated vehicle interactively and observe pedal inputs and dynamics appear immediately as J1939 messages on a connected CAN analyzer, and inspect the signal mappings between BeamNG.Tech outputs and their corresponding PGN/SPN definitions.

4 Use Cases and Future Work

Accessible Vehicle Security Datasets. The platform enables generation of large volumes of labeled CAN data without physical vehicle access. Simulation scenarios can be precisely instrumented with ground-truth labels — vehicle state, driver behavior, environmental conditions — that are difficult to obtain reliably from physical test collection.

Safe Cyberattack Simulation. A planned extension will integrate CAN injection capability, enabling attack effects on vehicle dynamics and driver response to be studied in a closed-loop environment without risk to personnel or equipment. The original DriverID dataset included a live CAN injection attack during each drive [3]; reproducing this in simulation will enable IDS evaluation and attack detection studies at scale, complementing existing real-vehicle datasets [4].

Open-Source Release. All middleware source code, J1939 signal mapping definitions, and simulation scenario configurations will be released publicly to provide a reusable foundation for the research community.

5 Related Work

The challenge of obtaining realistic, labeled vehicle CAN data for security research is well documented. Verma et al. [4] present the ROAD dataset, a comprehensive real-vehicle CAN intrusion dataset collected on an automotive dynamometer, and survey the limitations of existing datasets. Existing simulation approaches for automotive security research have largely relied on synthetic CAN traffic generators or hardware-in-the-loop benches [5], neither of which captures the full coupling between vehicle dynamics and bus state that characterizes real driving data. To our knowledge, no prior work has used a physics-based vehicle simulation engine to generate standards-compliant J1939 CAN traffic for cybersecurity research purposes.

6 Conclusion

We present a working middleware connecting BeamNG.Tech to a physical CAN network via real-time J1939 generation, enabling vehicle cybersecurity research without physical vehicle access or proprietary signal databases. With 22 DriverID-aligned signals implemented and transmitting live J1939 traffic, the platform provides an immediate foundation for simulation-based driving behavior and security studies. CAN injection support and an open-source release will follow.

References

[1] BeamNG GmbH. BeamNG.Tech: Research and engineering simulation platform. https://beamng.tech, 2024.

[2] SAE International. SAE J1939: Serial control and communications heavy duty vehicle network. Technical standard, SAE International, 2022.

[3] E. Reid, S. Powers, E. Gallegos, J. Daily, T. Biggs, and T. Lanigan. ORNL Driver Identification Dataset. ORNL Constellation, 2025. doi:10.13139/ORNLNCCS/2513388.

[4] M. E. Verma, R. A. Bridges, M. D. Iannacone, S. C. Hollifield, P. Moriano, S. C. Hespeler, B. Kay, and F. L. Combs. A comprehensive guide to CAN IDS data and introduction of the ROAD dataset. *PLOS ONE*, 2024. doi:10.1371/journal.pone.0296879.

[5] C. Young, J. Olufowobi, G. Bloom, and J. Zambreno. Intrusion detection system for the CAN bus: Survey and directions. In *Proc. IEEE ICESS*, 2019.