Intrusion Detection Systems in Autonomous Vehicles Using Machine Learning

Authors : Hashim Babat, Nirangan Dangi, Anish Dabhane

Abstract : As autonomous vehicles (AVs) and the Internet of Vehicles (IoV) transform transportation, ensuring the security of vehicular networks is crucial. Increased connectivity through Vehicle-to-Everything (V2X) technology exposes both intra-vehicle (CAN) and external networks to cyber-attacks. This survey examines state-of-the-art Intrusion Detection Systems (IDS) designed to counter threats like DoS, message injection, spoofing, and sniffing attacks. We focus on key IDS frameworks—Multi-Tiered Hybrid IDS (MTH-IDS), Tree-Based IDS, and Leader Class Confidence Decision Ensemble (LCCDE)—that leverage machine learning models such as decision trees, ensemble learning, XGBoost, and LightGBM. Their performance on datasets like CICIDS2017 and CAN-Intrusion is compared based on detection accuracy, false alarms, and real-time feasibility. We also discuss challenges such as computational limits and propose future directions, including advanced ML and blockchain, to enhance AV and IoV security.

Keywords : autonomous vehicles, internet of vehicles, V2X, CAN, intrusion detection systems, cyber-attacks, decision trees, ensemble learning, gradient-boosting, XGBoost, LightGBM, CAN-intrusion, zero-day attacks
Conference Title : ICCSCIT 2025 : International Conference on Computer Science, Cybersecurity and Information Technology
Conference Location : New Delhi, India
Conference Dates : February 24-25, 2025

Open Science Index, Computer and Information Engineering Vol:19, No:02, 2025 publications.waset.org/abstracts/197694.pdf