

Author

Licence

Fatim Sbai

CC BY 4.0

New Vistas

Volume 12, Issue 1, 2026, UWL Annual Doctoral Students' Conference 2025

Abstract

In vehicular ad-hoc networks (VANETs), ensuring the reliability of vehicle-to-vehicle communications, requires robust intrusion detection systems (IDS) capable of identifying malicious behaviours. One of the main challenges in developing reliable solutions for vehicular networks is identifying a representative dataset that comprehensively captures all types of misbehaviours. Many existing datasets either lack diversity, are outdated, or do not accurately reflect real-world conditions. This makes it difficult to ensure that all potential attack scenarios are properly represented and evaluated, ultimately impacting the reliability and generalisation of the developed approaches.

The VeReMi dataset is a widely recognised benchmark that attempts to address these issues, featuring various simulated misbehaviours such as Constant Position, Constant Offset, Random Position, Random Offset, and Eventual Stop attacks. While attacks like Constant and Random Positions are relatively easy to detect due to their erratic nature, more subtle attacks, including Constant Offset and Eventual Stop, closely mimic legitimate behaviours, making detection significantly more challenging. Additionally, the dataset's naturally imbalanced distribution, where attack instances are vastly outnumbered by benign traffic, further complicates detection.

To address this imbalance, the project focuses exclusively on oversampling techniques to enhance minority class representation, deliberately avoiding undersampling to preserve valuable benign data. Conventional methods, such as Synthetic Minority Over-sampling Technique (SMOTE) and Adaptive Synthetic Sampling (ADASYN), improve class balance but often fail to capture the underlying complexity of subtle attacks. In contrast, more recent approaches based on Generative Adversarial Networks (GANs), including Conditional GANs (CGANs) and Wasserstein GANs (WGANs), demonstrate superior capabilities in synthesising realistic and diverse minority instances. Leveraging these advances, the project adopts CGAN-based oversampling to better model the nuanced behaviours present in vehicular networks, thereby enhancing the IDS's ability to detect both obvious and subtle misbehaviours with greater generalisation and robustness. In doing so, it aims to enhance intrusion detection systems with improved generalisation and robustness, ultimately supporting researchers in developing more scalable and effective solutions for real-world VANET environments.

Keywords

vehicular ad-hoc networks, vehicle-to-vehicle communications, VeReMi dataset, Conditional GANs