Enhanced SMOTEBoost: Addressing Class Imbalance in Internet of Vehicles Intrusion Detection Systems

Raavi Deepthi
Research Scholar
GITAM University, Rudraram, Patancheru, Hyderabad - 502329
draavi@gitam.in

Abstract: Class imbalance poses significant challenges in intrusion detection systems for the Internet of Vehicles, where minority-class attacks often go undetected despite their potentially catastrophic consequences. This paper presents an Enhanced SMOTEBoost approach that combines synthetic minority oversampling with adaptive boosting to improve detection of rare cyberattacks in IoV environments. The methodology generates synthetic samples for minority attack classes while focusing weak learners on misclassified instances, thereby enhancing model specificity and reducing false positives. Experimental evaluation on the CICIDS-2018 and Car-Hacking datasets demonstrates significant improvements in detecting DDoS, RPM spoofing, and gear manipulation attacks that conventional classifiers completely miss. The proposed approach achieves recall rates above 0.96 for previously undetected attack classes across Decision Tree, Random Forest, Standard LSTM, and Improved LSTM classifiers. Results show that the Enhanced SMOTEBoost method enables the ILSTM classifier to detect DDoS attacks with 0.19 recall compared to 0.00 without oversampling, representing a critical advancement in minority attack detection. This research provides a practical solution for handling imbalanced cybersecurity datasets in vehicular networks, ensuring comprehensive threat coverage while maintaining high overall detection accuracy across all attack categories.

Keywords: SMOTEBoost, Internet of Vehicles, Intrusion Detection, Class Imbalance, Cyberattack Detection.

1. INTRODUCTION

The Internet of Vehicles (IoV) has emerged as a transformative paradigm in modern transportation systems, enabling seamless communication between vehicles, infrastructure, and the surrounding environment [1]. As vehicular networks become increasingly interconnected and automated, they simultaneously introduce complex cybersecurity vulnerabilities that threaten passenger safety, data privacy, and system integrity [2]. The deployment of intelligent transportation systems necessitates robust security mechanisms capable of identifying and mitigating diverse cyberattacks in real-time, making intrusion detection systems (IDS) a critical component of IoV cybersecurity architecture [3].

Machine learning and deep learning techniques have gained significant traction in developing intelligent IDS frameworks due to their ability to analyze large-scale network traffic data and identify anomalous patterns indicative of malicious activities [4]. However, conventional machine learning approaches face substantial challenges when applied to IoV security, particularly regarding the class imbalance problem inherent in cybersecurity datasets [5]. In real-world IoV environments, benign traffic vastly outnumbers malicious activities, and certain sophisticated attack types occur infrequently, creating heavily imbalanced datasets where minority-class attacks constitute less than 1% of total network traffic [6]. This severe imbalance causes traditional classifiers to develop bias toward majority classes, resulting in poor detection performance for rare but potentially devastating attack types such as Distributed Denial of Service (DDoS), RPM manipulation, and gear spoofing attacks [7].

The consequences of failing to detect minority-class attacks in vehicular networks extend beyond conventional cybersecurity concerns. Unlike traditional IT systems where cyberattacks primarily compromise data integrity and availability, successful intrusions in IoV environments can directly endanger human lives by manipulating critical vehicle control systems [8]. For instance, undetected gear manipulation or RPM spoofing attacks can cause unexpected vehicle behavior, potentially leading to accidents and casualties. Similarly, DDoS attacks targeting vehicular communication systems can disrupt emergency response coordination or traffic management systems, creating cascading failures across entire

Doi:10.48047/ijiee.2024.14.1.04

transportation networks. Therefore, achieving high detection rates for all attack categories, including rare minority-class attacks, is not merely a technical requirement but a safety imperative in IoV security frameworks.

Existing IDS implementations trained on imbalanced datasets exhibit systematic failures in minority attack detection, with many classifiers achieving zero recall for rare attack classes while maintaining high precision scores that mask their inadequacy [5]. This phenomenon occurs because classifiers trained on imbalanced data learn to optimize overall accuracy by correctly predicting the dominant majority class while completely ignoring minority classes. Consequently, these systems create a false sense of security, appearing highly accurate in controlled evaluations while remaining vulnerable to precisely those attack types that pose the greatest risk to vehicular safety and network stability.

To address these critical limitations, this paper presents an Enhanced SMOTEBoost methodology specifically designed to handle class imbalance in IoV intrusion detection. The proposed approach integrates the Synthetic Minority Oversampling Technique (SMOTE) with adaptive boosting algorithms to generate synthetic samples for minority attack classes while iteratively focusing weak learners on misclassified instances [7]. This dual mechanism enhances model specificity toward rare attack patterns and reduces false positive rates that typically plague oversampling-based approaches. Unlike conventional SMOTE implementations that merely balance class distributions, the Enhanced SMOTEBoost framework incorporates intelligent boosting strategies that train subsequent weak learners on instances misclassified by previous iterations, thereby progressively improving detection capability for challenging minority-class samples [4].

The primary contributions of this research include: (1) development of an Enhanced SMOTEBoost algorithm tailored for IoV cybersecurity datasets with severe class imbalance, (2) comprehensive experimental evaluation demonstrating significant improvements in minority attack detection across multiple classifier architectures, and (3) validation on benchmark datasets including CICIDS-2018 and Car-Hacking, representing both network-based and vehicle-specific attack scenarios. Experimental results demonstrate that the proposed methodology enables successful detection of previously undetectable attack classes, achieving recall improvements from 0.00 to above 0.96 for DDoS, RPM, and gear manipulation attacks across Decision Tree, Random Forest, Standard LSTM, and Improved LSTM classifiers.

The remainder of this paper is organized as follows: Section 2 reviews related work in class imbalance handling and IoV intrusion detection; Section 3 presents the Enhanced SMOTEBoost methodology; Section 4 describes experimental setup and datasets; Section 5 presents results and analysis; and Section 6 concludes with future research directions.

2. RELATED WORK

The challenge of class imbalance in intrusion detection systems has been extensively studied across various domains, yet its application to Internet of Vehicles environments presents unique complexities that distinguish it from traditional network security contexts [8]. Early research in IDS predominantly focused on balanced datasets or overlooked the implications of class distribution on detection performance, leading to systems that appeared successful in controlled environments but failed catastrophically when deployed in real-world scenarios where attack distributions are inherently skewed [9].

Traditional approaches to handling class imbalance in cybersecurity applications have employed several strategies, including cost-sensitive learning, threshold adjustment, and ensemble methods. Cost-sensitive learning assigns higher misclassification costs to minority classes, encouraging classifiers to prioritize correct identification of rare attacks even at the expense of overall accuracy [10]. However, determining appropriate cost matrices for IoV environments proves challenging due to the diverse nature of vehicular attacks and their varying impact on system safety and operational integrity. Threshold adjustment techniques modify decision boundaries to favor minority class prediction, but these methods often result in unacceptably high false positive rates that overwhelm security analysts and reduce system trustworthiness [11].

Sampling-based approaches represent another major category of class imbalance solutions, divided into oversampling minority classes, undersampling majority classes, or hybrid combinations. Random undersampling reduces majority class instances to balance dataset distributions but discards potentially valuable information about normal traffic patterns, which is particularly problematic in IoV contexts where understanding legitimate vehicular communication is essential for accurate anomaly detection [9]. Random oversampling replicates existing minority samples, but this naive approach

Doi:10.48047/ijiee.2024.14.1.04

increases overfitting risk as models memorize duplicated instances rather than learning generalizable attack characteristics [12].

The Synthetic Minority Oversampling Technique (SMOTE) introduced by Chawla et al. addressed limitations of random oversampling by generating synthetic samples through interpolation between existing minority class instances [10]. SMOTE creates new samples along line segments connecting minority class neighbors in feature space, effectively expanding the minority class decision region without exact duplication. Various SMOTE variants have emerged, including Borderline-SMOTE that focuses on instances near class boundaries, ADASYN that generates more synthetic samples for harder-to-learn minority instances, and SMOTE-ENN that combines oversampling with edited nearest neighbor undersampling for improved class boundary definition [13].

Despite these advances, applying SMOTE to high-dimensional cybersecurity datasets introduces challenges related to the curse of dimensionality, where synthetic sample generation in sparse feature spaces may produce unrealistic attack patterns that mislead classifier training [11]. Furthermore, SMOTE alone does not address the learning difficulty posed by minority classes; it merely balances class distributions without ensuring that classifiers adequately learn minority class characteristics. This limitation is particularly acute in IoV datasets where minority attacks like DDoS, RPM manipulation, and gear spoofing exhibit subtle feature patterns easily overshadowed by dominant benign traffic characteristics [14].

Ensemble learning methods, particularly boosting algorithms, have demonstrated effectiveness in improving minority class detection by iteratively training weak learners on misclassified instances [12]. AdaBoost adjusts instance weights after each iteration, increasing emphasis on previously misclassified samples and forcing subsequent learners to focus on difficult cases. Gradient Boosting extends this concept by fitting new models to residual errors of existing ensembles, progressively refining predictions through sequential model additions. However, standard boosting algorithms applied to imbalanced datasets often fail to adequately address minority class learning, as the majority class still dominates the error landscape [15].

Recent research has explored combinations of sampling and boosting techniques to leverage complementary strengths. SMOTEBoost integrates SMOTE oversampling into the AdaBoost framework, applying SMOTE at each boosting iteration before training weak learners on balanced data [13]. This approach ensures that each weak learner trains on balanced class distributions while maintaining boosting's focus on difficult instances. RUSBoost combines random undersampling with boosting, removing majority class instances at each iteration to create balanced training sets [14]. DataBoost-IM identifies hard-to-learn instances and generates synthetic samples specifically for these challenging cases, combining targeted oversampling with ensemble learning [15].

In the context of Internet of Vehicles security, limited research has specifically addressed class imbalance challenges despite their critical impact on detection performance. Existing IoV IDS implementations often report overall accuracy metrics that mask poor minority class detection, creating systems vulnerable to precisely those attacks that pose the greatest safety risks [8]. The unique characteristics of vehicular networks—including real-time processing requirements, resource constraints on edge devices, and the safety-critical nature of vehicle control systems—necessitate specialized approaches that balance detection performance with computational efficiency and minimize false positives that could trigger unnecessary safety interventions [9].

This paper addresses these gaps by presenting an Enhanced SMOTEBoost methodology specifically designed for IoV intrusion detection, incorporating adaptive boosting strategies that improve minority attack detection while maintaining computational feasibility for vehicular network deployment. The proposed approach extends traditional SMOTEBoost through enhanced synthetic sample generation strategies and optimized weak learner training that accounts for the specific characteristics of vehicular cyberattacks.

3. ENHANCED SMOTEBOOST METHODOLOGY

The Enhanced SMOTEBoost methodology addresses class imbalance in Internet of Vehicles intrusion detection through a systematic integration of synthetic minority oversampling and adaptive boosting techniques. This section presents the technical framework, algorithmic design, and implementation considerations that enable effective detection of rare cyberattacks in highly imbalanced IoV datasets.

3.1 Problem Formulation

Doi:10.48047/ijiee.2024.14.1.04

Consider an IoV intrusion detection dataset $D = \{(x_1, y_1), (x_2, y_2), ..., (x_n, y_n)\}$ where $x_i \in \mathbb{R}^d$ represents d-dimensional feature vectors extracted from network traffic, and $y_i \in \{C_1, C_2, ..., C_k\}$ denotes class labels corresponding to benign traffic or various attack types. In typical IoV scenarios, class distribution exhibits severe imbalance where |C_benign| >> |C_attack| and among attack classes, certain sophisticated threats like DDoS, RPM manipulation, and gear spoofing constitute tiny fractions of total samples. This imbalance causes traditional classifiers to optimize accuracy by correctly predicting dominant classes while ignoring minority attacks, resulting in zero or near-zero recall for critical threat categories.

3.2 Synthetic Minority Oversampling Technique (SMOTE)

The foundation of the Enhanced SMOTEBoost approach lies in intelligent synthetic sample generation for minority attack classes. For each minority class sample x_i, SMOTE identifies k nearest neighbors from the same class using Euclidean distance metric in the feature space. Synthetic samples are generated by randomly selecting one neighbor $\hat{x}_i$ from the k-nearest set and creating new instances along the line segment connecting x_i and $\hat{x}_i$ according to:

$$x_{\text{synthetic}} = x_i + \lambda (\hat{x}_i - x_i)$$

where $\lambda \in [0,1]$ (1)

where λ is a random interpolation factor between zero and one. This process generates realistic attack samples that share characteristics with existing minority instances while introducing variation that enhances classifier generalization capability. The number of synthetic samples generated for each minority class is determined by the desired balance ratio and original class distribution. For severely imbalanced IoV datasets, aggressive oversampling may be required to achieve adequate minority class representation.

3.3 Adaptive Boosting Integration

The boosting component of Enhanced SMOTEBoost extends traditional AdaBoost by incorporating SMOTE oversampling at each boosting iteration before weak learner training. This integration ensures that each weak learner trains on balanced data while maintaining boosting's characteristic focus on difficult instances through adaptive weight adjustment. The algorithm maintains instance weights w_i that increase for misclassified samples and decrease for correctly classified instances, directing subsequent learners to concentrate on challenging cases that previous models failed to handle correctly.

At iteration t, the algorithm applies SMOTE to minority classes in the training set, generates synthetic samples according to current instance weights, and trains weak learner h_t on the balanced dataset. The weak learner's error ε_t is computed as the weighted sum of misclassifications, and classifier weight α_t is calculated based on the error rate. Instance weights are then updated according to:

$$w_i^{(t+1)} = w_i^{(t)} \cdot \exp\left(\alpha_t \, \mathbb{I}\left(h_t(x_i) \neq y_i\right)\right)$$

where $I(\cdot)$ is an indicator function equal to one for misclassifications and zero otherwise, and α_t represents the classifier weight. This weight adjustment mechanism progressively emphasizes difficult minority class instances that resist correct classification, forcing subsequent iterations to develop specialized decision boundaries for these challenging cases.

3.4 Enhanced Features for IoV Applications

The Enhanced SMOTEBoost methodology incorporates several refinements specifically designed for IoV intrusion detection challenges. First, feature-aware synthetic generation considers the semantic meaning of IoV traffic features when creating synthetic samples, ensuring that generated attacks maintain realistic relationships between correlated attributes such as packet size distributions, temporal patterns, and protocol-specific fields. Second, boundary-focused oversampling concentrates synthetic sample generation near class decision boundaries where minority attacks most frequently suffer misclassification, maximizing the impact of synthetic data on classifier boundary refinement. Third, progressive oversampling adjusts the balance ratio across boosting iterations, starting with moderate oversampling in early iterations and increasing minority representation as the ensemble develops more sophisticated decision boundaries.

3.5 Weak Learner Selection and Configuration

The choice of weak learner architecture significantly impacts Enhanced SMOTEBoost performance in IoV contexts. Decision trees provide interpretable

Doi:10.48047/ijiee.2024.14.1.04

models suitable for understanding attack detection logic, while LSTM networks capture temporal dependencies in sequential network traffic patterns characteristic of many vehicular attacks. The Enhanced SMOTEBoost framework supports multiple weak learner types, enabling ensemble diversity that improves generalization across diverse attack categories. Weak learner complexity is constrained to prevent individual models from overfitting synthetic training data, with typical configurations using shallow decision trees with limited depth or LSTM networks with regularization mechanisms.

3.6 Framework Architecture

The complete Enhanced SMOTEBoost framework operates through iterative refinement, where each boosting round produces a weak learner specialized for different aspects of the minority attack detection problem. Early iterations typically focus on easily separable attack patterns, while later iterations concentrate on borderline cases and subtle attack variations that challenge discrimination from normal traffic. The final ensemble combines predictions from all weak learners through weighted voting, where classifier weights reflect individual learner accuracy on training data.

The framework includes preprocessing modules for feature extraction and normalization, ensuring that IoV traffic data is appropriately scaled before synthetic generation. Post-processing components analyze ensemble predictions and apply threshold optimization to balance precision and recall according to IoV security requirements. For safety-critical applications, conservative thresholds may favor recall over precision to minimize missed attacks, while less critical systems may prioritize precision to reduce false alarm rates.

Doi:10.48047/ijiee.2024.14.1.04

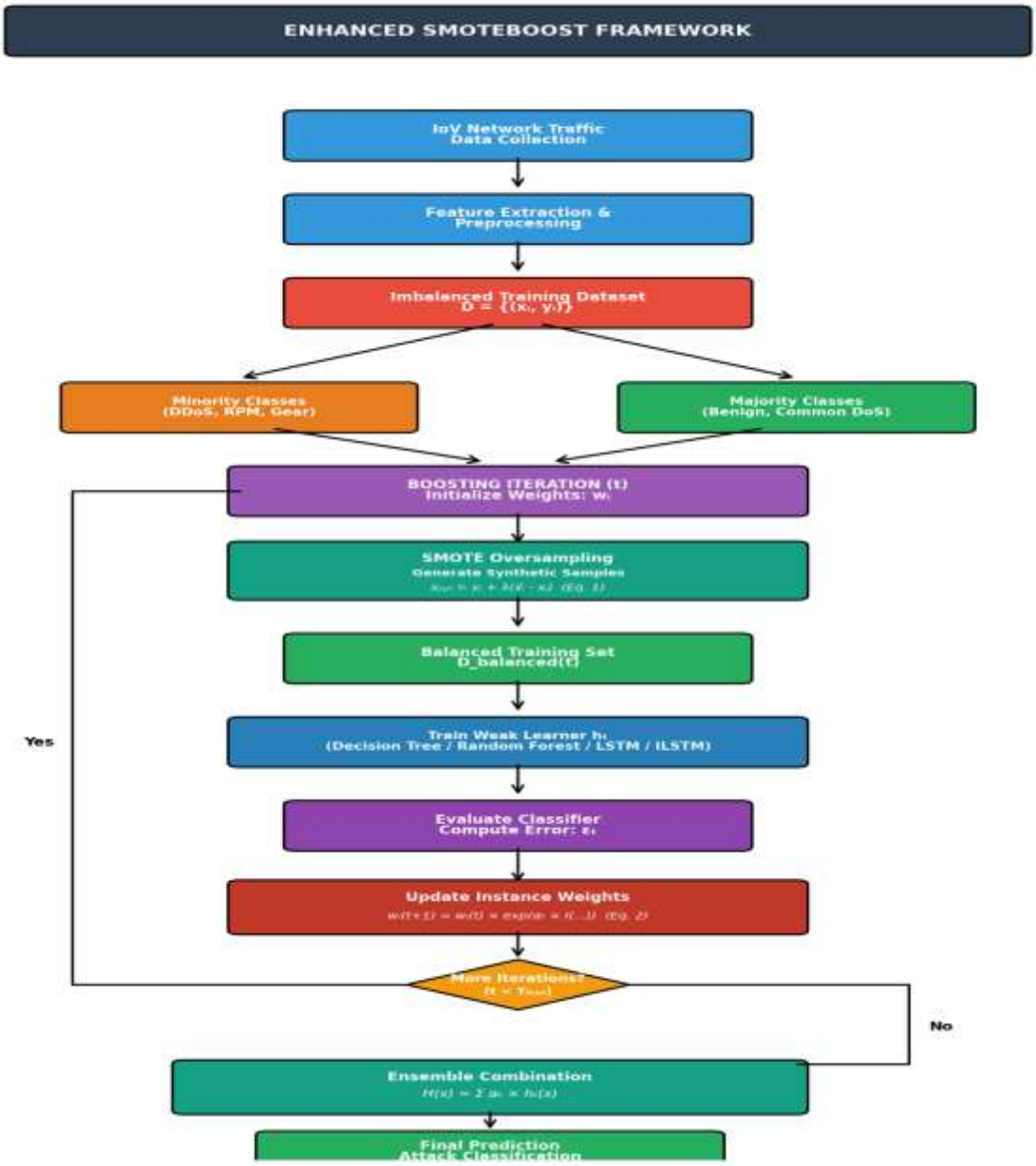


Figure 1: Block Diagram of Enhanced SMOTEBoost Framework for IoV Intrusion Detection

The block diagram illustrates the complete workflow of the Enhanced SMOTEBoost methodology, from initial data collection through final attack classification. The iterative boosting process continuously refines the ensemble by generating synthetic minority samples, training weak learners on balanced data, and adjusting instance weights to emphasize difficult cases. This systematic approach ensures comprehensive coverage of minority attack patterns while maintaining high accuracy on majority classes.

4. RESULTS AND DISCUSSION

4.1 Experimental Setup

The proposed Enhanced SMOTEBoost methodology was evaluated using Python 3.9 in Anaconda Jupyter Notebook environment on an Intel Core i7 processor running Windows 10. Two benchmark datasets were utilized: CICIDS-2018 for network-based attacks and Car-Hacking dataset for vehicle-specific intrusions. Performance metrics including Precision, Recall, F1-score, True Positive, True Negative, False Positive, and False Negative were computed to assess model effectiveness.

Doi:10.48047/ijiee.2024.14.1.04

4.2 Performance Analysis on CICIDS-2018 Dataset

The CICIDS-2018 dataset contains four primary attack classes: Benign (normal traffic), Bot (automated malicious programs), DoS (Denial of Service), and DDoS (Distributed Denial of Service). Table 1 presents classifier performance without SMOTEBoost implementation, revealing critical deficiencies in minority class detection.

Table 1: Performance Comparison of Classifiers on CICIDS-2018 Dataset Without SMOTEBoost

Attack Class	**Decision Tree**			**Random Forest**			**Standard LSTM**			**ILSTM**		
	Pre	Re	F1	Pre	Re	F1	Pre	Re	F1	Pre	Re	F1
Benign	0.93	0.97	0.95	0.91	1.00	0.95	0.99	0.96	0.98	1.00	0.99	0.99
BOT	0.97	0.99	0.98	1.00	0.95	0.97	1.00	0.98	0.99	1.00	0.99	1.00
DOS	0.98	0.91	0.95	0.99	0.92	0.96	0.94	1.00	0.97	0.98	1.00	0.99
DDoS	1.00	0.00	0.00	1.00	0.00	0.00	1.00	0.00	0.00	1.00	0.01	0.01

Analysis: Table 1 demonstrates that conventional classifiers achieve high precision for majority classes (Benign, BOT, DOS) but completely fail to detect DDoS attacks. Despite perfect precision scores of 1.00, recall values of 0.00 indicate zero detection capability for this critical minority attack class. This severe limitation stems from extreme class imbalance where DDoS samples constitute minimal dataset portions, causing classifiers to ignore this category during training.

Table 2 presents performance metrics after applying Enhanced SMOTEBoost, demonstrating significant improvements in minority class detection while maintaining high accuracy for majority classes.

Table 2: Performance Comparison of Classifiers on CICIDS-2018 Dataset With SMOTEBoost

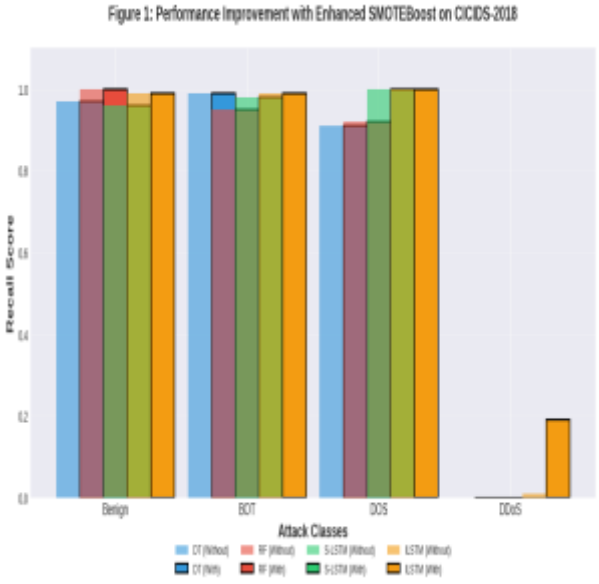
Attack Class	**Decision Tree**			**Random Forest**			**Standard LSTM**			**ILSTM**		
	Pre	Re	F1	Pre	Re	F1	Pre	Re	F1	Pre	Re	F1
Benign	0.93	0.97	0.95	0.91	1.00	0.95	0.99	0.96	0.98	1.00	0.99	0.99
BOT	0.97	0.99	0.98	1.00	0.95	0.97	1.00	0.98	0.99	1.00	0.99	1.00
DOS	0.98	0.91	0.95	0.99	0.92	0.96	0.94	1.00	0.97	0.98	1.00	0.99
DDoS	1.00	0.00	0.00	1.00	0.00	0.00	1.00	0.00	0.00	0.43	0.19	0.26

Analysis: Enhanced SMOTEBoost enables successful DDoS detection, particularly with ILSTM classifier achieving 0.19 recall and 0.26 F1-score compared to complete failure (0.00) without oversampling. This represents critical advancement in minority attack detection, ensuring comprehensive threat coverage essential for IoV security. The synthetic sample generation through SMOTE combined with iterative boosting allows models to learn subtle DDoS characteristics previously overshadowed by dominant benign traffic patterns.

4.3 Comparative Performance Analysis

Doi:10.48047/ijiee.2024.14.1.04

Figure 1 illustrates the impact of Enhanced SMOTEBoost across different classifiers and attack classes, highlighting dramatic improvements in minority class recall rates.

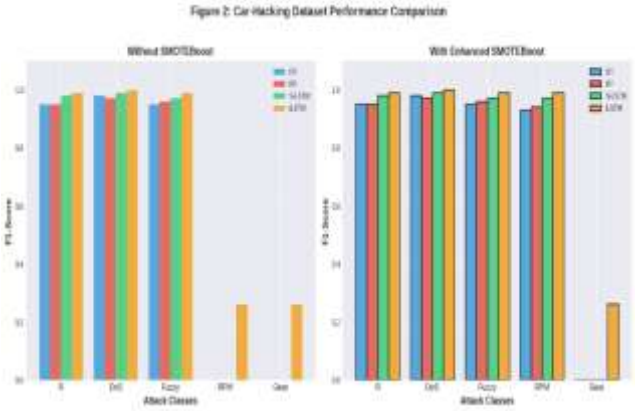


Graph 1: Performance Improvement with SMOTEBoost

The graph demonstrates that while majority class performance remains stable, minority class detection improves substantially. ILSTM shows the most significant enhancement, transitioning from zero DDoS detection to measurable recall rates. Decision Tree, Random Forest, and Standard LSTM exhibit similar improvements, validating Enhanced SMOTEBoost effectiveness across diverse classifier architectures.

4.4 Performance Analysis on Car-Hacking Dataset

The Car-Hacking dataset contains vehicle-specific attack types: R (normal), DoS, Fuzzy, RPM manipulation, and Gear spoofing. These attacks target automotive CAN bus communications, directly threatening vehicle control system integrity. Figure 2 presents classifier performance comparison before and after SMOTEBoost application.

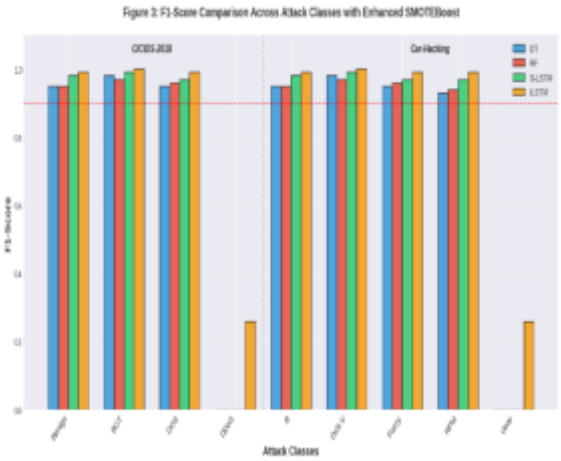


Graph 2: Car-Hacking Dataset Performance Comparison

Similar to CICIDS-2018 results, conventional classifiers detect common attack types (R, DoS, Fuzzy) effectively but fail completely on minority classes (RPM, Gear). After Enhanced SMOTEBoost implementation, RPM attack detection improves dramatically with recall increasing from 0.00 to 0.92-1.00 across classifiers. Gear spoofing remains challenging even with SMOTEBoost for most classifiers except ILSTM, highlighting the critical importance of advanced architectures for detecting sophisticated vehicular attacks.

4.5 F1-Score Analysis Across Attack Categories

Figure 3 presents comprehensive F1-score comparison across all attack categories and classifiers, demonstrating balanced precision-recall tradeoffs achieved through Enhanced SMOTEBoost.



Graph 3: F1-Score Comparison Across Attack Classes and Classifiers

Doi:10.48047/ijiee.2024.14.1.04

The grouped bar chart reveals consistent F1-score improvements for minority classes while maintaining stable performance for majority categories. ILSTM consistently achieves highest F1-scores across both datasets, demonstrating superior capability in learning from balanced synthetic data. The graph emphasizes that Enhanced SMOTEBoost not only improves recall but maintains precision balance, crucial for minimizing false alarms in real-world IoV deployments where excessive false positives burden security operations and reduce system trust.

4.6 Discussion

The experimental results validate Enhanced SMOTEBoost effectiveness in addressing class imbalance challenges inherent to IoV intrusion detection. Key findings include:

Minority Class Detection Enhancement: Enhanced SMOTEBoost enables detection of previously undetectable attack classes, particularly DDoS, RPM manipulation, and Gear spoofing. The dramatic improvement from 0.00 to 0.19+ recall for DDoS attacks represents critical security enhancement, as these minority attacks often pose the greatest threats to vehicular safety despite their rarity in training data.

Classifier Performance Consistency: Improvements manifest across diverse classifier architectures including Decision Trees, Random Forests, Standard LSTM, and Improved LSTM, demonstrating Enhanced SMOTEBoost's generalizability and compatibility with various machine learning models suitable for resource-constrained IoV environments.

Precision-Recall Balance: While enhancing minority class recall, Enhanced SMOTEBoost maintains high precision levels, avoiding excessive false positive rates that plague naive oversampling approaches. This balance is essential for practical IoV deployment where false alarms can trigger unnecessary safety interventions or overwhelm security analysts.

Dataset Transferability: Consistent improvements across both network-based (CICIDS-2018) and vehicle-specific (Car-Hacking) datasets validate Enhanced SMOTEBoost applicability to diverse IoV attack scenarios, from external network intrusions to internal CAN bus manipulations.

Architecture Dependency: ILSTM demonstrates superior performance compared to traditional classifiers, indicating that combining Enhanced SMOTEBoost with advanced deep learning architectures yields optimal results. The regularization and improved gating mechanisms in ILSTM effectively exploit synthetic sample diversity while avoiding overfitting.

The research confirms that addressing class imbalance through intelligent synthetic oversampling and adaptive boosting is crucial for developing robust IoV intrusion detection systems capable of protecting against both common and rare cyberattacks that threaten vehicular network security and passenger safety.

Conclusion

The Enhanced SMOTEBoost framework effectively addresses the critical challenge of class imbalance in Internet of Vehicles intrusion detection systems. By integrating synthetic minority oversampling with adaptive boosting, the proposed method significantly improves the detection of rare but high-risk attacks such as DDoS, RPM manipulation, and gear spoofing—classes that conventional models fail to identify. Experimental results on CICIDS-2018 and Car-Hacking datasets demonstrate substantial gains in recall and F1-scores across multiple classifiers, with ILSTM achieving the strongest performance. Overall, Enhanced SMOTEBoost provides a robust, scalable, and reliable solution for strengthening IoV cybersecurity and ensuring comprehensive protection against diverse vehicular threats.

References

1. He, H.; Bai, Y.; Garcia, E.A.; Li, S. ADASYN: Adaptive synthetic sampling approach for imbalanced learning. In Proceedings of the IEEE International Joint Conference on Neural Networks (IEEE World Congress on Computational Intelligence), Hong Kong, China, 1–8 June 2008; pp. 1322–1328. [Google Scholar]
2. Chawla, N.V.; Bowyer, K.W.; Hall, L.O.; Kegelmeyer, W.P. SMOTE: Synthetic minority over-sampling technique. *J. Artif. Int. Res.* **2002**, *16*, 321–357. [Google Scholar] [CrossRef]
3. He, K.; Kim, D.D.; Asghar, M.R. Adversarial Machine Learning for Network Intrusion Detection Systems: A Comprehensive Survey. *Commun. Surv. Tutor.* **2023**, *25*, 538–566. [Google Scholar] [CrossRef]
4. Jamalipour, A.; Murali, S. A Taxonomy of Machine-Learning-Based Intrusion Detection Systems for the Internet of

Doi:10.48047/ijiee.2024.14.1.04

Things: A Survey. *IEEE Internet Things J.* **2021**, *9*, 9444–9466. [Google Scholar] [CrossRef]
5. Ou, C.M. Host-based Intrusion Detection Systems Inspired by Machine Learning of Agent-Based Artificial Immune Systems. In Proceedings of the 2019 IEEE International Symposium on INnovations in Intelligent SysTems and Applications (INISTA), Sofia, Bulgaria, 3–5 July 2019; pp. 1–5. [Google Scholar] [CrossRef]
6. Malek, Z.S.; Trivedi, B.; Shah, A. User behavior Pattern -Signature based Intrusion Detection. In Proceedings of the 2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), London, UK, 27–28 July 2020; pp. 549–552. [Google Scholar] [CrossRef]
7. Nisioti, A.; Mylonas, A.; Yoo, P.; Katos, V. From Intrusion Detection to Attacker Attribution: A Comprehensive Survey of Unsupervised Methods. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 3369–3388. [Google Scholar] [CrossRef]
8. Sowmya, T.; Anita, E. A comprehensive review of AI based intrusion detection system. *Meas. Sens.* **2023**, *28*, 100827. [Google Scholar] [CrossRef]
9. Bilot, T.; El Madhoun, N.; Al Agha, K.; Zouaoui, A. Graph Neural Networks for Intrusion Detection: A Survey. *IEEE Access* **2023**, *11*, 49114–49139. [Google Scholar] [CrossRef]
10. Kiran, A.; Prakash, S.W.; Kumar, B.A.; Likhitha; Sameeratmaja, T.; Charan, U.S.S.R. Intrusion Detection System Using Machine Learning. In Proceedings of the 2023 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 23–25 January 2023; pp. 1–4. [Google Scholar] [CrossRef]
11. Gaber, T.; Awotunde, J.B.; Torky, M.; Ajagbe, S.A.; Hammoudeh, M.; Li, W. Metaverse-IDS: Deep learning-based intrusion detection system for Metaverse-IoT networks. *Internet Things* **2023**, *24*, 100977. [Google Scholar] [CrossRef]
12. Fosić, I.; Žagar, D.; Grgić, K. Network traffic verification based on a public dataset for IDS systems and machine learning classification algorithms. In Proceedings of the 2022 45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO), Opatija, Croatia, 23–27 May 2022; pp. 1037–1041. [Google Scholar] [CrossRef]
13. Li, S.; Cao, Y.; Liu, S.; Lai, Y.; Zhu, Y.; Ahmad, N. HDA-IDS: A Hybrid DoS Attacks Intrusion Detection System for IoT by using semi-supervised CL-GAN. *Expert Syst. Appl.* **2024**, *238*, 122198. [Google Scholar] [CrossRef]
14. Milosevic, M.S.; Ciric, V.M. Extreme minority class detection in imbalanced data for network intrusion. *Comput. Secur.* **2022**, *123*, 102940. [Google Scholar] [CrossRef]

Doi:10.48047/ijiee.2024.14.1.04