**Network Intrusion Detection in VANETS Using Machine Learning: Securing VANETS With Machine Learning- Based NIDS Approach**

I. Ravi Prakash Reddy 1, Akshaya Juluri2, Sanjana Reddy3, Pola Rishika 4

1Professor, Department of Information Technology, G. Narayanamma Institute of Technology and Science for Women Hyderabad, India

irpreddy@test.gnits.ac.in1, juluriakshaya03@gmail.com2,rsanjana090@gmail.com3, rishikapola157@gmail.com3

1Corresponding Email Id: irpreddy@test.gnits.ac.in

**Abstract.** In response to the growing cybersecurity challenges in Vehicular Ad Hoc Networks (VANETs), we designed a Network Intrusion Detection System (NIDS) based on machine learning that can better detect malicious threats. The system is based on three main algorithms: Random Forest, XGBoost, Gradient Boosting. These algorithms classify network traffic as normal or malicious. By combining these algorithms, the system exploits their collective strengths, thereby improving the detection accuracy. The NIDS has an alert function that sends notifications about possible intrusions directly to the user's web interface. This approach will improve road safety and traffic management by strengthening vehicular communication security. The system is trained and evaluated using the NLS-KDD dataset for better detection performance in VANET environments.

**Keywords:** Network Intrusion Detection System (NIDS), Vehicular Ad Hoc Networks (VANETS), NSL-KDD Dataset, Machine Learning Algorithms, Ensemble Learning, Alert Systems.

1. Introduction

In the last few years, VANETs have emerged as an important part of smart cities, allowing for advanced communication systems such as V2V and V2I [1]. V2V allows direct communication between vehicles, while V2I connects vehicles to roadside infrastructure, such as traffic lights, optimizing traffic flow and improving road safety [1]. These innovations play a crucial role in developing intelligent transportation systems to reduce congestion, minimize accidents, and have safer roads. Despite these advances, VANETs are susceptible to cyber threats, which compromise communication and potentially endanger driver safety [4]. This vulnerability points to the imperative necessity for stringent security measures that can protect the reliability and integrity of VANETs.

To counter these vulnerabilities, this project introduces the development of a Network Intrusion Detection System (NIDS) especially designed for VANETs. The system uses machine learning algorithms such as Random Forest Classifier, XGBoost, and Gradient Boosting to classify network traffic as either normal or malicious [3]. By integrating these algorithms through ensemble learning, the NIDS benefits from their individual strengths, improving detection accuracy and reducing false positives [7]. They mostly tend to fail to manage computational complexity and dynamic topologies in networks [3-9]

In addition, the system employs an alerting mechanism that keeps the users of any possible intrusions through a simple web inter-face for effective reactions to threats [2].

2 Literature Review

In the year 2023, Adithya and Ravish [8] proposed a VANET-based intrusion detection system to identify false messages in the network. Their paper uses machine learning techniques for the classification and filtering of erroneous communication that originates from malicious sources to ensure network reliability. In the same year, 2024, Palaniappan et al. [9] used an enhanced Dynamic Source Routing (DSR) protocol combined with machine learning methods for the detection of malicious nodes in VANETs. This has improved the detection and isolation of malicious nodes to contribute to a more secure communication environment in VANETs.

In 2023, Kawale et al. [10] proposed a framework for the detection of malicious activity in VANETs by using both traditional detection techniques and modern machine learning algorithms to classify traffic as either normal or malicious.. Meanwhile, in 2021, Gonçalves et al. [11] assessed several VANET datasets in terms of their effectiveness in intrusion detection systems. Their study gives insights into the challenges of using these datasets in real-world scenarios, such as handling large amounts of data.

In addition, in 2021, Ercan et al. [12] proposed a machine learning-based system for detecting position falsification attacks in VANETs. Their work focuses on detecting misbehavior related to position falsification, which can undermine the credibility of communication in VANETs, thereby highlighting the importance of secure and accurate positioning within these networks.

3 Proposed System

In our proposed system, we introduced a novel approach in enhancing the security of VANETs (Vehicular Ad Hoc Networks) using a Network Intrusion Detection System (NIDS) powered by ensemble machine learning techniques. By combining algorithms like Random Forest, XGBoost, and Gradient Boosting, the system enhances detection accuracy while minimizing false positives. Additionally, it incorporates a alert system integrated with a web interface, enabling prompt notifications and responses to potential threats. This project focuses on securing vehicular communication from attacks.

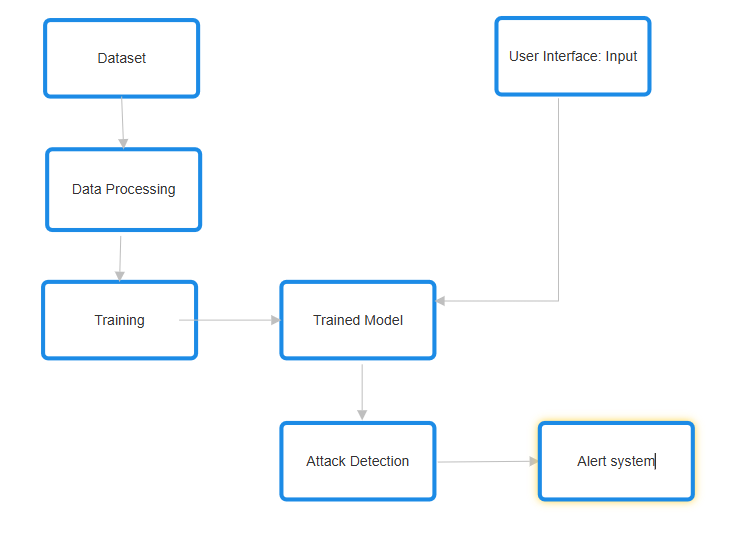
****

Figure.1. System Architecture

In figure 3.1, the System architecture portraying the pipeline for a machine learning-based network intrusion detection system (NIDS) in vehicular ad hoc networks (VANETs). The architecture starts with a dataset, which goes through data processing to prepare it for the model training. This data after processing is used to train a machine learning model. The trained model is integrated to web interface. The user has to provide input through the user interface, which interacts with the trained model in identifying possible malicious activities. Upon detecting an attack, the system triggers an alert system to notify users or the concerned administrator for intervention, thus enhancing the security of vehicular communication networks.

**3.1. PROPOSED MODEL ALGORITHM**

**Algorithm:**

1. Import required libraries pandas, numpy for data handling, LabelEncoder, SimpleImputer, SMOTE for preprocessing, RandomForestClassifier, GradientBoostingClassifier, XGBClassifier for modeling, accuracy\_score, classification\_report, and confusion\_matrix for evaluation, streamlit for deploying the web application.

2. Load and preprocess dataset and remove duplicates, handle missing values, encode categorical data using LabelEncoder.

3.: Extract a subset of features relevant for the model feature selection, set target variable and split the dataset into training and testing sets using train\_test\_split.

4. Handle class imbalance using Synthetic Minority Oversampling Technique (SMOTE) to generate synthetic samples.

5. Train individual models by initializing the Random Forest Classifier model, Gradient Boosting Classifier model, XGBoost Classifier model and fit each model using the resampled training dataset.

6. For each base model, generate predictions, evaluate their performance and display the evaluation results.

7 Use Ensemble Blending for Final Model:

-Generate class probabilities for each model on the testing dataset.

-Weighted Blending: Combine probabilities using a weighted average formula.

-Final Predictions: select the class with the highest probability for each instance.

8. Evaluate Blended model:

-Compute metrics such as Accuracy, Classification Report, Confusion Matrix and print the evaluation results for the blended model.

9. Deployment using Streamlit:

-Create a user interface, preprocess inputs, predict based on user data, and display results.

**4 Results and Analysis**

#### In our work, we developed an Intrusion Detection System (IDS) for Vehicular Ad Hoc Networks (VANETs) leveraging machine learning to enhance security by detecting potential attacks. The system utilized the NSL-KDD dataset and implemented an ensemble approach combining Random Forest Classifier and Gradient Boosting**,** XGBoost algorithms, capitalizing on their robustness and precision in handling large-scale, imbalanced data. We got an accuracy of 93%, 93%, 95%, 96% for algorithms XGBoost, Random Forest Classifier, Gradient Boosting, and Ensemble approach(Blending) respectively as shown in figures 4.1 (a), (b), 4.2 (a), (b) respectively. The models were trained to classify network traffic as either normal or malicious, with a focus on accurately identifying common VANET attacks. We interfaced the ensemble model with web interface as shown in figure 4.3 (a). Upon detecting an attack, the system triggered an alert message as shown in figure 4.3 (b). This user-friendly interface provides immediate attack alerts to ensure swift action by administrators.

#### 

Figure 4.1 (a)Random Forest Classifier model performance metrics (b)XGBoost model performance metrics.

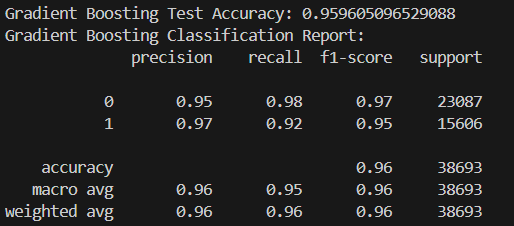
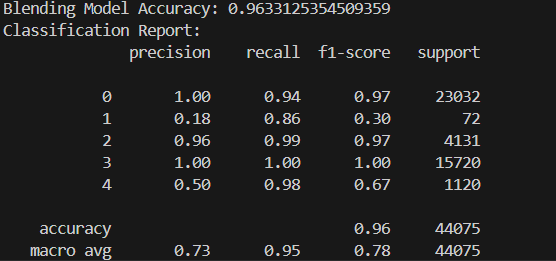
 

Figure 4.2. (a)Gradient Boosting model performance metrics (b) Ensemble approach (Blending) model performance metrics

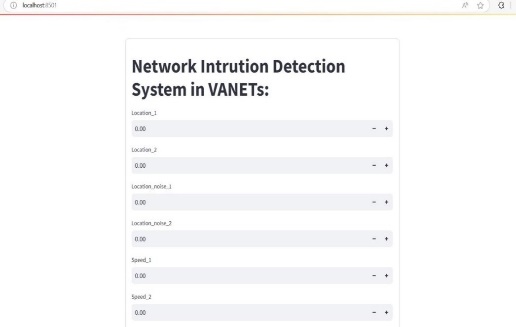
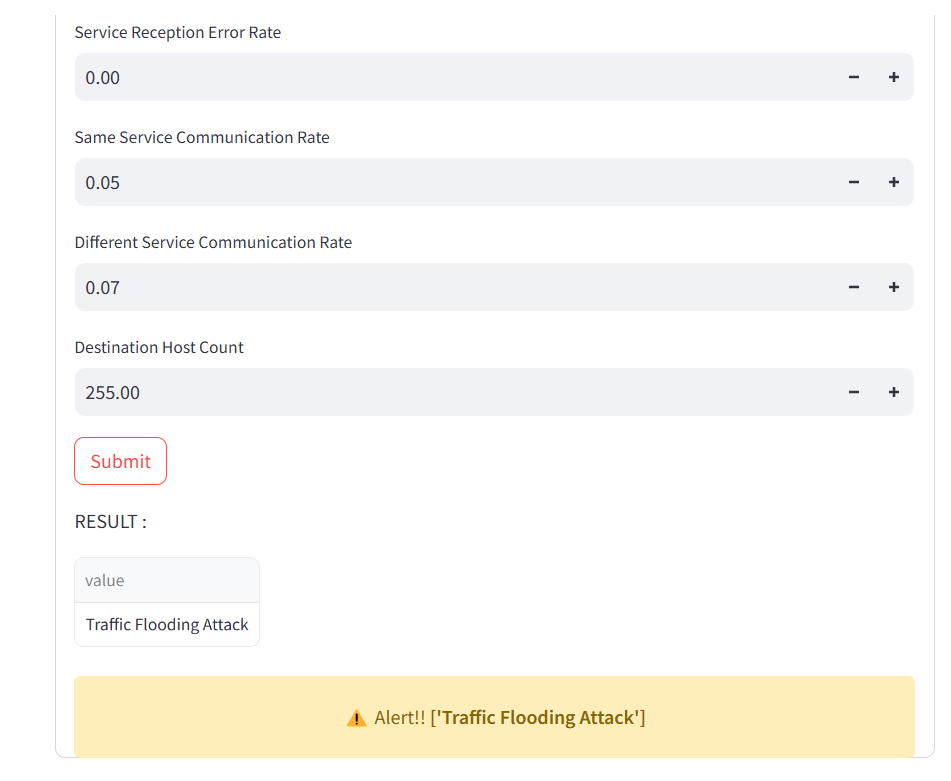
 

Figure 4.3. (a)Network Intrusion Detection System in Vanet’s Web Interface (b)Alert Message.

5 Conclusion and Future scope

In conclusion, developing a Network Intrusion Detection System (NIDS) for Vehicular Ad Hoc Networks is vital for enhancing the security of transportation systems. Our project utilizes machine learning algorithms to detect and classify the cyberattacks and network traffic efficiently. The use of ensemble learning techniques improves the detection accuracy while also minimizing the false positives. The alert system enables quick responses to security risks. Future developments for the NIDS can utilize real-time data from sensors and other sources to enhance threat detection.

**References**

[1] Kumar, A. B., & Singh, M. (2023, August). Enhancing Intrusion Detection in Autonomous Vehicles Using Tree-Based Machine Learning Techniques. In *2023 3rd Asian Conference on Innovation in Technology (ASIANCON)* (pp. 1-7). IEEE.

[2] Gad, A. R., Nashat, A. A., & Barkat, T. M. (2021). Intrusion detection system using machine learning for vehicular ad hoc networks based on ToN-IoT dataset. *IEEE Access*, *9*, 142206-142217.

[3] So, S., Sharma, P., & Petit, J. (2018, December). Integrating plausibility checks and machine learning for misbehavior detection in VANET. In *2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA)* (pp. 564-571). IEEE.

[4] Zang, M., & Yan, Y. (2021, April). Machine learning-based intrusion detection system for big data analytics in VANET. In *2021 IEEE 93rd vehicular technology conference (VTC2021-Spring)* (pp. 1-5). IEEE.

[5] Naqvi, I., & Chaudhary, A. (2021, September). Intrusion detection using soft computing techniques in VANETs. In *2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO)* (pp. 1-4). IEEE.

[6] Deng, C., & Qiao, H. (2016, October). Network security intrusion detection system based on incremental improved convolutional neural network model. In *2016 International Conference on Communication and Electronics Systems (ICCES)* (pp. 1-5). IEEE.

[7] Suliman, S. I., Abd Shukor, M. S., Kassim, M., Mohamad, R., & Shahbudin, S. (2018, April). Network intrusion detection system using artificial immune system (AIS). In *2018 3rd International Conference on Computer and Communication Systems (ICCCS)* (pp. 178-182). IEEE.

[8] Adithya, B. V., & Ravish, R. (2023, October). VANETs based Intrusion Detection System for False Message Identification. In *2023 First International Conference on Advances in Electrical, Electronics and Computational Intelligence (ICAEECI)* (pp. 1-7). IEEE.

[9] Palaniappan, A. N., Pranav, J., Shivamanikkavasakam, S., Kumar, S., & Gandhiraj, R. (2024, March). Malicious Node Detection in VANETs via Enhanced DSR and ML. In *2024 International Conference on Wireless Communications Signal Processing and Networking (WiSPNET)* (pp. 1-7). IEEE.

[10] Kawale, R. M., Patil, R. V., & Patil, L. V. (2023, August). Framework for Detecting Malicious Activity in Vehicular Ad hoc Network. In *2023 Second International Conference on Augmented Intelligence and Sustainable Systems (ICAISS)* (pp. 1407-1412). IEEE.

[11] Gonçalves, F., Macedo, J., & Santos, A. (2021, September). Evaluation of VANET datasets in context of an intrusion detection system. In *2021 International Conference on Software, Telecommunications and Computer Networks (SoftCOM)* (pp. 1-6). IEEE.

[12] Ercan, S., Ayaida, M., & Messai, N. (2021). Misbehavior detection for position falsification attacks in VANETs using machine learning. *IEEE Access*, *10*, 1893-1904.