Mesopotamian journal of Computer Science
Vol. 2024, **pp**. 122–133
DOI: https://doi.org/10.58496/MJCSC/2024/010 ; ISSN: 2958-6631
https://mesopotamian.press/journals/index.php/cs

Research Article

Enhancing Security and Performance in Vehicular Adhoc Networks: A Machine Learning Approach to Combat Adversarial Attacks

Mustafa Abdulfattah Habeeb [1, 2], Yahya Layth Khaleel [1,2, *], Ahmed Raheem Abdulnabi [3]

[1] *College of Computer Science and Mathematics, Tikrit University, Iraq*

[2] *Faculty of Mechanical Engineering and Informatics, University of Miskolc, H-3515 Miskolc, Hungary*

[3] *College of Business Informatics, University of Information Technology and Communications (UOITC), Baghdad, Iraq*

ARTICLE INFO

Article History
Received 10 Jun 2024
Revised: 18 Jul 2024
Accepted 01 Sep 2024
Published 20 Sep 2024

Keywords
Security
VANET
Networks
Machine Learning
Adversarial Attacks
Data Privacy
Threat Mitigation

ABSTRACT

Integrating Machine Learning (ML) techniques into Vehicular Adhoc Networks (VANETs) provides promising features in autonomous driving and ITS applications. In this paper, DSRC data is used to evaluate the effectiveness of different ML models, including Naive Bayes, Random Forest, KNN, and Gradient Boosting, in normal and adversarial scenarios. Since the dataset is relatively imbalanced, the Synthetic Minority Over-sampling Technique (SMOTE) is employed for sampling, and defensive distillation for improving model resilience to adversarial perturbations. From the results, it is clear that models such as Gradient Boosting and Random Forest show high accuracy in both cases, thus showing the potential of using Machine Learning to improve VANET security and reliability when new threats appear. Through this research, the significance of the application of ML in the protection of vehicular communication in order to enhance both traffic safety and flow has been articulated.

1. INTRODUCTION

In recent years, wireless communications that capable to support high mobility broadband communication have gotten more and more attention from both the academic and industrial fields [1- 4]. The development of networked vehicles has made remarkable progress in improving how vehicles share information. Devices within vehicles as well as the Onboard Units (OBU's) are critical for building an Intelligent Transportation System (ITS) and smart cities. Each car carries an OBU that communicates with other vehicles and with roadside equipment. We will soon see that vehicular networks shape our daily routines over the next few years [5, 6]. Our life will become less complicated and more secure through its advancements [7]. With the growth of technology and AI capabilities we can establish experiences for autonomous driving.

A special wireless mobile Adhoc network called vehicular Adhoc network (VANET) is emerged to support the vehicular wireless communication [8]. VANET is a type of Mobile Adhoc Network (MANET) [9]. VANET has been developed in recent years. The IEEE standard for the Figure 1: An illustration for a simple VANET concept.

*Corresponding author. Email: yahya@tu.edu.iq

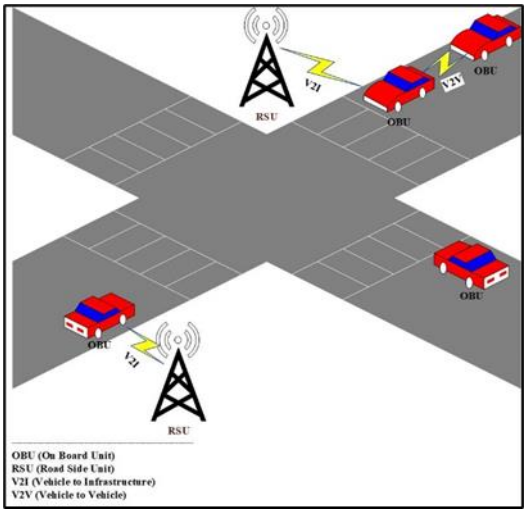

Fig. 1. A simple VANET concept [10].

In simple way, the VANET system consist of mobile nodes which have the sensors built in them called the On Board Units (OBU's), and fixed nodes located at the road side used to collect and send data called the Road Side Units (RSU's) [11]. The RSU's are permanent nodes functions as a gateway to the internet or a server to exchange information. Moreover, VANET has two types of communications, the first is the vehicle-to-vehicle communication (V2V) which connects mobile nodes among them, and the other is vehicle-to-infrastructure (V2I) which connects mobile nodes to the fixed nodes (RSU's) [12]. Nowadays, Artificial intelligence (AI) is becoming a transformative that can impact a lot of industries positive due to its characteristics in analyzing, processing [13-16] and making decision [17-20]. It incorporated into almost every discipline, such as health [21], business [22], transportation [23], climate [24], languages [25], production, teaching, and many others with an objective to optimize its functioning, working, interaction, and outcome [26-28]. AI has received attention in research as useful in enhancing system reliability in disasters and in the assessment of forensic evidence. Moreover, exposure to fake news and improvement of societal safety utilizing AI employs all elements of the artificial capacity to overcome social issues [29,30]. Moreover, In the domain of cybersecurity, AI finds itself rather essential. That is why it can be considered highly effective tool for pattern recognition, identification of specific weaknesses, and real-time reactions to various forms of adversarial attacks [31]. Anywhere AI needed to become important since it is meaningfully used to protect information and to ensure the stability of the digital environment to prevent malware, phishing and hacking [27][32]. While AI technology advances, so does its position in the construction of a safer, stronger external environment.

Machine learning became one of the most dominant technologies that controls today's technical equipment [33-35]. Areas from medicine, agriculture, advertisements, communications, etc. are integrated with machine learning to deliver best experience to the user [36-39]. VANET, which uses the wireless communications as a major technology to connects nodes with each other so as to deliver data among nodes within the network, is in need to use faster and reliable today's artificial intelligence technologies so as to deliver best experience to its decision maker's nodes in order to make best decision [40].These decisions provide safety of environment and traffic management which are considered the most important goals of using VANET. Machine learning has different methods to implement so as to get a better output result with in the field. These methods are divided into three divisions [41], Supervised Machine Learning (SML), Unsupervised Machine Learning, and Reinforced Machine Learning. All the aforementioned categories have two stages of implementation which are training and testing. In training stage, the machine learning model trained based on a given dataset, while in testing stage, the model is tested to give a prediction for a futuristic input[41]. SML employs various algorithms with a labeled dataset in order to come up with a better model [42]. These algorithms are subdivided into two groups: classification algorithms and regression algorithms. Classification algorithms such as k-nearest neighbor [43], Bayesian classifiers [44], decision trees [45], neural networks [46], and support vector machine [47] are used to train the model to predict a categorical output for a category labeled input. Regression algorithms such as logistic regression [48], support vector regression [49], and gaussian process for regression [44] are used to train the model to predict a numerical output for a numerical labeled input. Unsupervised learning approach has the ability to use unlabeled data set to achieve an efficient representation of data set's samples without labeling the information. Clustering and dimension reduction are two cases of unsupervised learning. Clustering, in which data samples are grouped in a cluster of data samples that have a similarity in behavior, is a representative state of unsupervised learning. In clustering, the samples within a particular cluster have a similarity in behavior while other clusters have different samples with different behavior. The conventional algorithms used in clustering are hierarchical clustering [50], k-means [51], spectrum clustering [52], and Dirichlet process [53]. Dimension reduction, also known as dimensionality

reduction is a technique used in unsupervised learning to perform feature selection or extraction. The aim of using this technique is to find the important features that can be used for prediction. Dimension reduction saves more storage and reduces the time needs to make a decision. Some conventional algorithms used in dimension reduction are the linear projection methods, like principles component analysis [54] and nonlinear projection methods, like local linear embedding [55], manifold learning [56], and isometric feature mapping [57]. In reinforcement learning, the limitation of solving multi-step problems is solved. A trial and error are used in this type of learning to solve the problems. An agent is used to interact with the environment to achieve a multi-step goal within the environment. The objective of the agent is to learn how to always choose the right action that leads it closer to its goal. The Markov decision process (MDP) models the environment to introduce action and rewards to a Markov process. Sarsa [58] and Q-learning algorithms can be used in reinforcement learning to solve the problems. The temporal variation of wireless communication in VANET can be handled using reinforcement learning.

Machine learning are susceptible to various kinds of attacks which is called adversarial attack.

The aim behind using VANET is to provide safer road driving, more economical trip, and less pollution environment. To achieve the previously mentioned aims, a VANET should have a secured communication as it uses a wireless based communication which in turn is vulnerable to external attacks by outsiders [59]. In a VANET, there are different kinds of attacks, figure 2 shows these types of attacks [60].

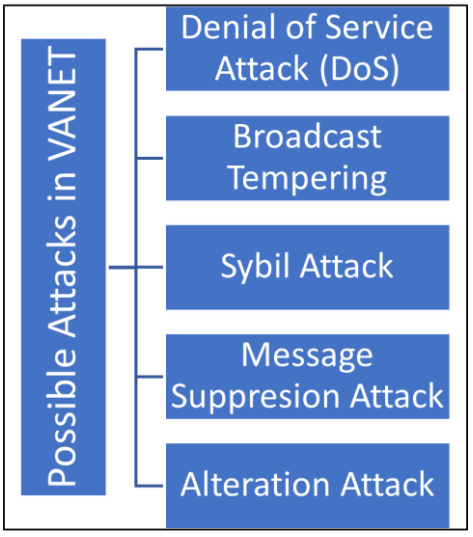

Fig. 2. Possible attacks in a VANET

In DOS attack [61] the attacker tries to flood the network with legitimate large number of packets. The network will be overwhelmed in a way that that server node cannot handle the capacity of the packets anymore, which leads to dropping packets.

Broadcast tempering is an attack tries to inject messages filled with false information related to the road's blockage, incorrect safety messages, wrong information related to traffic jams in order to deceive the network to make them make a wrong decision.

In sybil attack, the attacker uses the identity of legitimate nodes and forges them for his own purposes. These forged identities deceive the network and show the network that there are more vehicles than the actual number on the road. Also, the attacker sends false information about the position and direction information [62].

Suppression attack is another type of attack where the attacker selects some packets by sniffing them through the communication channels, and drops some packets that may content significant and substantial information for the receiver [63]. The attacker takes a copy of these packets after suppressing them, and this copy of packets used by the attacker when required. The aim behind this attack is to prohibit the authorities from taking updates about vehicles positions and collisions if happened. Also, it prevents the delivery of collision report to the RSUs.

Finally, in alteration attack, the attacker modifies the content of the targeted packets. The attacker sniffs the information from the communication channel and then modifies the information by altering their header and body of packets [64], [65]. Alteration attack can be implemented by different methods, either by replaying recent messages, or by delaying the transmission of packets, or modifying the data of transmitted information.

2. METHODOLOGY AND RESULTS

Machine Learning is just like another tool, vulnerable to adversarial attacks which can have huge implications in a world where we trust them with human lives via self-driving cars and other automation [66-68]. This work tries to say that: the ML learning models must be tradeoff between accuracy and robustness. Refer to figure 3.

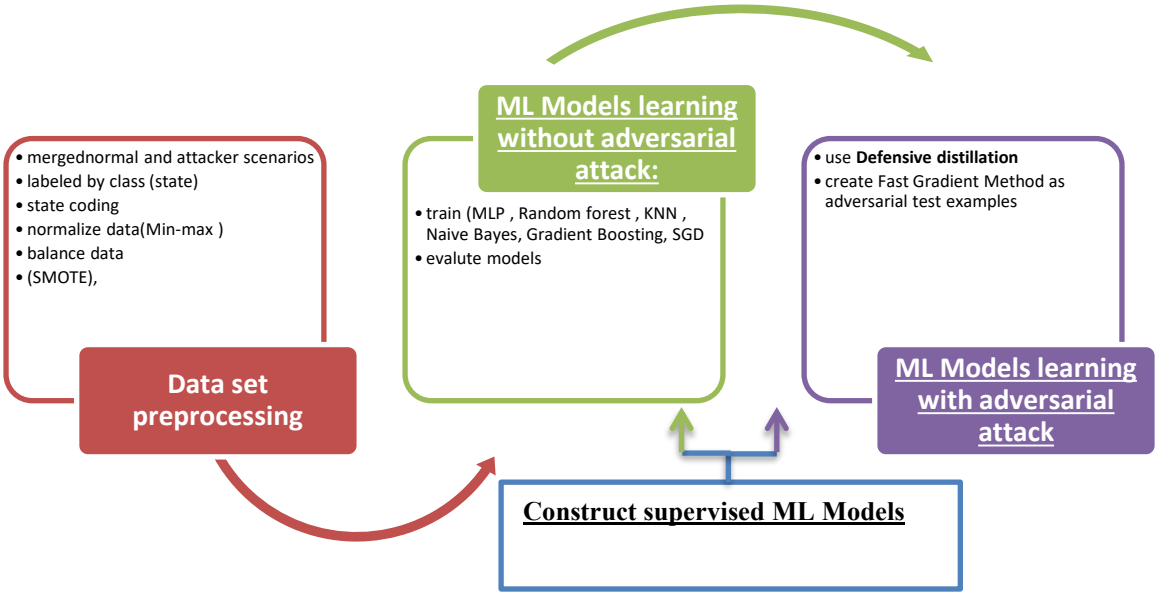

Fig. 3. Proposed methodology

2.1 Data set description

Dedicated short-range communication (DSRC) dataset offers data concerning wireless communications between vehicles and road side units. two isolated data sets are provided (normal scenario) and in the presence of attacker (jammer)." Communications were setup based on IEEE 802.11p standards at 5.9Ghz. 10BSM (Basic Service messages) per second. Using Control Channel (Ch172) a 10 Mhz channel. Also Attached a clean version in spreadsheets for each dataset (jammed and normal)". the dataset have (390 Instances) with no missing data

The typical data set comprises the non-Attacker scenario with [Highway (70-80Mph)] (RSU 1) (bi-directional data-exchange) (UDP packet size 500 byte) (Channel Bandwidth = 10 Mhz) (Data-Rate = 6Mbps) and counts vehicles from (1 10 20 40 60 80 100).

In a jamming situation Responsive-Intruder Scenario on a Highway (25-35Mph) with one RSU (multipoint data transmission) (UDP data packets of 500 bytes) (10 MHz channel bandwidth) (6 Mbps data rate) using up to 100 vehicles.40,60,80 and 100) In jammer scenario Reactive-Attacker Scenario with [Highway (25-35Mph)] (1 RSU) (bi-directional data-exchange) (UDP packet size 500 byte) (Channel Bandwidth = 10 Mhz) (Data-Rate = 6Mbps) and number of cars equal to (1,10,20,40,60,80 and 100).

2.2 Data set preprocessing

The two datasets have the same attributes for both the normal and attacker scenarios. These attributes are merged into one dataset. the dataset then labeled by addition one class called (state) field presenting the type of scenario (normal, attacker) where the code 0 is given for normal and code 1 for the attacker scenario. The following table presents the mutual features:

TABLE I. THE MUTUAL FEATURES

Fields name	***description***
Car P-Received	*Represents the power received by the car during communication, measured in dBm.*
Car-PDR (%)	*Packet Delivery Ratio (PDR) for the car, showing the percentage of successfully delivered packets.*
RSU PDSR (%)	*Packet Delivery Success Ratio (PDSR) for the Road Side Unit (RSU), expressed as a percentage.*

Car Received power (dBm)	*The amount of power received by the car during communication, in decibel-milliwatts (dBm).*
RSU-PDR (%)	*Packet Delivery Ratio (PDR) for the Road Side Unit (RSU), indicating successful packet transmission.*
number of OBU's	*The number of On-Board Units (OBUs) involved in communication.*
state	*Scenario label indicating whether the data corresponds to a normal (0) or jammer (attacker) (1) scenario.*

2.2.1 Normalization

Application of normalization is common in data preparation for machine learning [69]. By normalizing numeric columns in the dataset to a common scale; the team ensures the differences in value ranges remain unaffected.

One of the most frequent methods to normalize dataset is min-max normalization. One approach transforms every feature's minimum value into a 0 while its maximum value turns into a 1; all other values are mapped to values within the range of 0 and 1 according to a formula:

$$\frac{\text{value} - \text{min}}{\text{max} - \text{min}} \quad \ldots (1)$$

2.2.2 Data set balancing

In the dataset a great disparity exists in class representation as one category contains many samples (0 normal) while the other has limited examples (1 attacker). Classifiers strive to decrease total error rates rather than examining the distribution of the data. The balance has to be restored using data sampling.

After labeling (DSRC) dataset the distribution of state class has normal scenario equal to (322) and attacker class equal to (68) as shown in figure 4. this present imbalance dataset and could be biased to the majority class when ML models are trained. Refer to table 2 and 3.

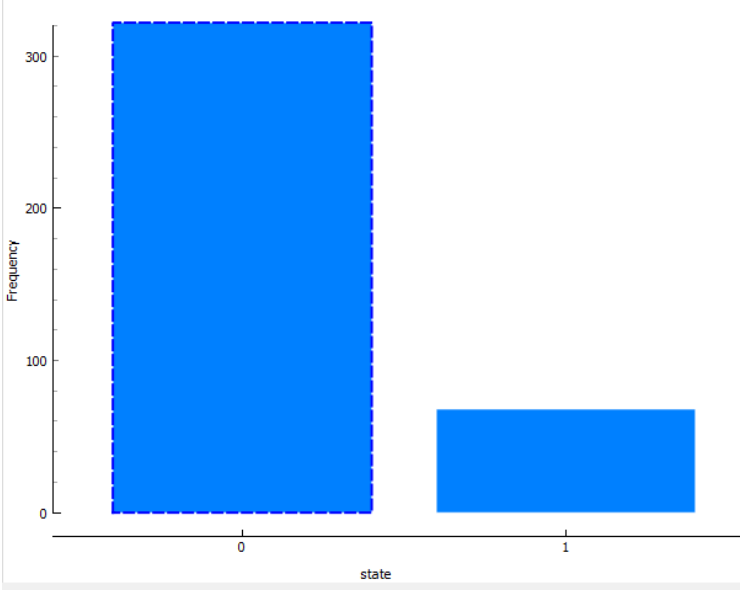

Fig. 4. Class distribution before use SMOTE

TABLE II. THE DATASET CLASSES BEFORE BALANCE

state	***No. of instances***
0(normal)	*322*
1(attacker)	*68*
	390

To bypass this problem Synthetic Minority Over-sampling Technique (SMOTE) was adopted [2]. It is an over-sampling technique whereby synthetic minority examples are generated. It combines informed oversampling of the minority class with random under-sampling of the majority class. The dataset distribution after balance become as that presented in figure 5:

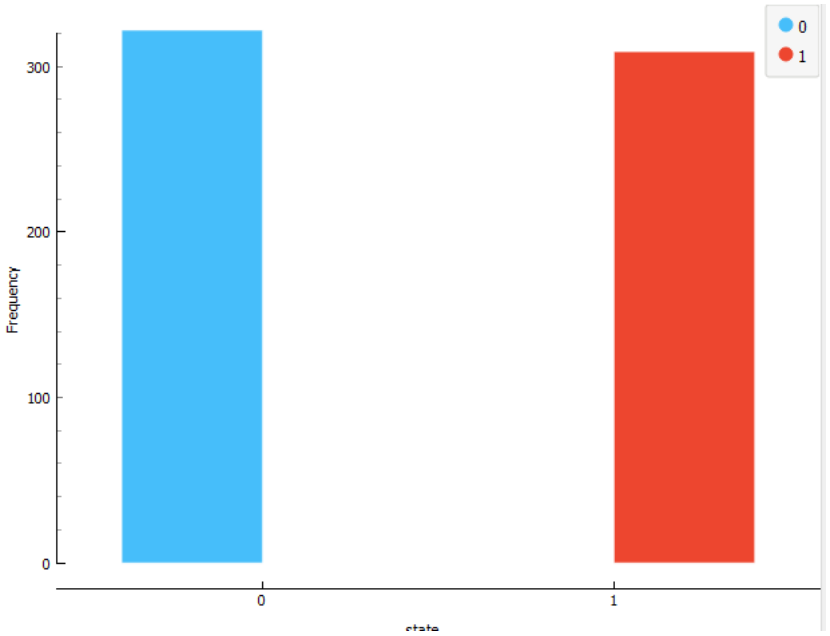

Fig. 5. Class distribution after use SMOTE

As a results of over sampled the number of dataset instances are increased.

TABLE III. THE DATASET CLASSES AFTER BALANCE

state	*No. of instances*
0(normal)	*322*
1(attacker)	*309*
	631

2.3 Construct supervised ML Models

Our work proposed a defense approach to train bunch of machine learning models normally without adversarial attack and then these models is feed to train with adversarial examples by using Defensive distillation approach. The work on defense leads into the idea of making machine learning models more robust in general.

2.4 ML Models learning without adversarial attack

The following ML models were trained without adversarial attack learning (without defense).these models are (MLP, Random forest, KNN, Naive Bayes, Gradient Boosting, SGD). The following steps is followed for learning procedure:

- Step 1: preprocessing of DSRC dataset, finalist with balanced data of 631 instance
- Step 2: learn the model without adversarial attack learning
  - Train the data set with (MLP, Random Forest, KNN, Naive Bayes, Gradient Boosting, SGD).
  - Test the dataset with evaluation metrics (Train time, Test time, accuracy).

The output of evaluation metrics is shown in table (4)

TABLE IV. RESULTS OF ML MODELS WITHOUT ADVERSARIAL ATTACK

ML Model	*Train time [s]*	*Test time [s]*	*accuracy*
Naive Bayes	*0.072*	*0.013*	*0.9017433*
SGD	*0.093*	*0.013*	*0.9698891*
Neural Network	*4.182*	*0.018*	*0.9698891*
KNN	*0.071*	*0.051*	*0.9809826*

Gradient Boosting	*1.143*	*0.02*	*0.9936609*
Random Forest	*0.223*	*0.033*	*0.9920761*

SGD and neural network has the same value in term of accuracy while Train time in SGD is less than in Neural Network. Gradient Boosting and Random Forest has the highly accuracy compared with other models while Naive Bayes has the lower accuracy compared to all models.

The purpose of this step is to calculate the accuracy of each model to compare it later when training the same model with adversarial attack example (with defense)

2.5 ML Models learning with adversarial attack example

Adversarial training is an intuitive defense method against adversarial samples, which attempts to improve the robustness of a neural network by training it with adversarial samples. Defensive distillation defenses that have been proposed in this work.

The work trained machine learning models on the DSRC dataset and creates adversarial examples using the Fast Gradient Sign Method. Here the ART classifier were used later to train the model. Adversarial Robustness Toolbox (ART) is a Python library for Machine Learning Security provides tools that enable developers and researchers to defend and evaluate Machine Learning models and applications against the adversarial threats of Evasion, Poisoning, Extraction, and Inference [70].

There are many techniques to create adversarial examples. Most approaches suggest minimizing the distance between the adversarial example and the instance to be manipulated, while shifting the prediction to the desired (adversarial) outcome. Some methods require access to the gradients of the model, which of course only works with gradient based models such as neural networks, other methods only require access to the prediction function, which makes these methods model-uncertain

2.6. Adversarial defenses

By training a backup model with a smoother surface in the schemes attackers usually aim to exploit we hinder their ability to reveal input changes leading to wrong categorization. The reason this method succeeds is that unlike the first system the second model uses soft probabilities from the main model instead of binary labels. Some success in protecting against initial variants of adversarial attacks was demonstrated by this technique.

The same ML models were trained with Fast Gradient Method as adversarial test examples. The following steps is followed for learning procedure:

- Step 1: Instantiate classifiers (MLP, Random forest, KNN, Naive Bayes, Gradient Boosting, and SGD)
- Step 2: fit on training data
- Step 3: Create the ART classifier
- Step 4: Train the ART classifier
- Step 5: Evaluate the ART classifier on benign test examples
- Step 6: Generate adversarial test examples
- Step 7: Evaluate the ART classifier on adversarial test examples

TABLE V. RESULTS OF ML MODELS ADVERSARIAL DEFENSES

ML Model	*Train time [s]*	*Test time [s]*	*Accuracy on benign test examples*	*Accuracy on adversarial test examples*
KNN	**2.052**	**0.921**	**99.3670%**	**98.2341%**
MLP (neural network)	**6.157**	**1.911**	**98.7341%**	**98.4012%**
RF	**0.989**	**0.180**	**99.3670%**	**97.4683%**
GB	**1.954**	**0.985**	**99.2145%**	**96.1453%**
SGD	**1.028**	**0.518**	**96.1525%**	**95.1281%**
Naive Bayes	**1.52**	**1.012**	**0.9103%**	**90.1715%**

As we note in the above (table 5), the training and test time will certainly increase, due to the learning of the ML models with the adversarial test examples that the model may be exposed to. the model compute Accuracy on benign test examples and Accuracy on adversarial test examples. Even neural network has the higher accuracy but train time is increased and accuracy decreased as consequence to model robustness .as noticed all Accuracy values' on adversarial test examples were decreased compared to Accuracy on benign test examples.

3. DISCUSSION

Data from the experiments reveals crucial understanding of using machine learning algorithms for VANETs from adversariaCl assaults. Analysis of these findings emphasizes essential features of model performance against attacks and their effectiveness in practical settings.

3.1 Model Accuracy and Robustness

The high accuracy of Gradient Boosting and Random Forest models is noteworthy under benign and dangerous conditions. The results illustrate that these models perform well in spotting and addressing potential dangers such as jamming and Sybil attacks in VANETs. Their impressive accuracy reveals their capacity to improve the security of VANET systems in adverse scenarios. The relatively small drop in accuracy for these models when exposed to adversarial examples (Gradient Boosting: 99.Their robustness is evident in the drop of the Gradient Boosting model from 99.21% to 96.14%, indicating its effectiveness for environments facing Security threats.

Naive Bayes and SGD demonstrated inferior accuracy together with decreased resistance to adversarial changes. The performance of Naive Bayes fell enormously in benign and adversarial contexts with just 90.17% accuracy. Although Naive Bayes might simplify training speed it is deficient in the strength essential for critical applications like VANETs.

3.2 Compromises exist between performance and precision

The results show a major conflict between accuracy and efficiency. Although MLP and Gradient Boosting gained high performance their training processes were notably slower than Naive Bayes and SGD. Naive Bayes and Random Forest took much less time to train compared to the Neural Network that took 6.157 seconds. Delay in training could be a major obstacle in applications that demand fast performance for secure car connectivity.

The analysis reveals that while Gradient Boosting and Neural Networks offer significant accuracy benefits their computational demands could require enhancements for immediate VANET scenarios. The Random Forest model strikes a favorable trade-off between precision and performance which positions it well for use in VANET applications.

3.3 Handling Data Imbalance

Applying the Synthetic Minority Over-sampling Technique (SMOTE) to tackle class imbalance worked well. Should SMOTE not be used models may lean towards the dominant class resulting in inadequate adversarial attack detection. When the dataset was equalized the models improved their effectiveness across both normal and adversary scenarios achieving greater accuracy and more accurate generalization.

The importance of confronting data imbalance in cybersecurity contexts where threats may be uncommon but crucial for detection has been shown by this finding. By utilizing SMOTE alongside powerful machine learning techniques we can effectively address this problem in VANETs.

3.4 Significant practical applications wait for future endeavors

The findings show that machine learning algorithms like Gradient Boosting and Random Forest can greatly improve the safety of VANETs. The models can be utilized in vehicle communication systems to uncover and counteract adversarial threats to improve traffic safety and efficiency.

A number of domains require enhancement. The reduction in accuracy in adversarial scenarios shows the necessity for additional study on better adversarial defense methods. Wider use of attack vectors in adversarial training along with model aggregation could improve the robustness of protection against threats.

Immediate application in live vehicular scenarios is vital for measuring how well these models perform under fluid network environments. Research in the future should examine the feasibility of using edge computing to handle vehicular data live and shorten response times while strengthening machine learning defenses.

By adding more diverse attack scenarios to the dataset we can improve the universality of models in different types of VANET environments.

In all models tested Defensive distillation notably increased model resilience. As adversarial examples were presented the accuracy decreased slightly; nonetheless the decrease was manageable in models including KNN and Neural Networks. Despite being affected by adversarial examples KNN achieved an accuracy of 98.23% while Neural Networks experienced a 0.33% decrease.

The data reveals that adversarial techniques can lower model accuracy while defensive distillation serves as a practical method to reduce this loss. Gradient Boosting and Random Forest demonstrated higher reductions in accuracy in response to adversarial situations. Armed with this insight researchers might find value in developing sophisticated adversarial defenses like incorporating various attack methods into adversarial training for better protection

4. CONCLUSION AND FUTURE WORK

This paper has demonstrated the potential of ML techniques in enhancing the security and performance of VANETs under both normal and adversarial conditions. By leveraging the DSRC dataset, we evaluated several ML models, including Random Forest, Gradient Boosting, and KNN, and assessed their effectiveness in detecting and mitigating threats such as jamming attacks. Our study addressed the challenges of data imbalance using the SMOTE technique and improved model resilience against adversarial perturbations through defensive distillation. The results indicated that models like Gradient Boosting and Random Forest achieved high accuracy, emphasizing the utility of ML in ensuring secure and reliable communications in VANETs. This research highlights the critical role of securing vehicular communication systems to promote traffic safety and enhance the resilience of autonomous driving technologies.

In future research, several avenues can be explored to extend this study. First, there is a need to investigate more advanced adversarial defense mechanisms, such as adversarial training with diverse attack vectors, to further improve the robustness of machine learning models against a wider array of cyber threats. Second, the real-time implementation of the proposed ML models in vehicular environments will be essential for assessing their performance under dynamic network conditions. Additionally, future work could involve the integration of deep learning models, such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), to enhance anomaly detection and prediction capabilities in vehicular networks.

Expanding the dataset by incorporating more diverse attack scenarios will also be crucial for generalizing the models' effectiveness across various vehicular environments. Finally, exploring the integration of edge computing can provide opportunities for real-time processing of vehicular data, improving scalability and reducing response times. These future directions will help strengthen the application of machine learning in VANETs, ensuring a safer, more reliable, and resilient vehicular network ecosystem

Funding
The author's paper explicitly states that no funding was received from any institution or sponsor.

Conflicts Of Interest
The author declares no conflict of interest in relation to the research presented in the paper.

Acknowledgment
The author would like to express gratitude to the institution for their invaluable support throughout this research project.

References

[1] X. Cheng, C. Chen, W. Zhang, and Y. Yang, “5G-Enabled Cooperative Intelligent Vehicular (5GenCIV) Framework: When Benz Meets Marconi,” IEEE Intell. Syst., vol. 32, pp. 53–59, 2017.

[2] S. DEVI, P. Maury, and U. N. Tripathi , Trans., “A Novel Method of Using Machine Learning Techniques to Protect Clouds Against Distributed Denial of Service (DDoS) Attacks”., Babylonian Journal of Machine Learning, vol. 2024, pp. 133–141, Aug. 2024, doi: 10.58496/BJML/2024/013.

[3] L. Liang, H. Peng, G. Y. Li, and X. Shen, “Vehicular communications: A physical layer perspective,” IEEE Trans. Veh. Technol., vol. 66, no. 12, pp. 10647–10659, 2017, doi: 10.1109/TVT.2017.2750903.

[4] Y. L. Khaleel, M. A. Habeeb, and H. Alnabulsi , Trans., “Adversarial Attacks in Machine Learning: Key Insights and Defense Approaches ”, Applied Data Science and Analysis, vol. 2024, pp. 121–147, Aug. 2024, doi: 10.58496/ADSA/2024/011.

[5] R. Zhang, X. Cheng, L. Yang, X. Shen, and B. Jiao, “A Novel Centralized TDMA-Based Scheduling Protocol for Vehicular Networks,” IEEE Trans. Intell. Transp. Syst., vol. 16, no. 1, pp. 411–416, 2015, doi: 10.1109/TITS.2014.2335746.

[6] X. Cheng, L. Yang, and X. Shen, "D2D for Intelligent Transportation Systems: A Feasibility Study," IEEE Trans. Intell. Transp. Syst., vol. 16, no. 4, pp. 1784–1793, 2015, doi: 10.1109/TITS.2014.2377074.

[7] L. Liang, H. Ye, and G. Y. Li, "Toward Intelligent Vehicular Networks: A Machine Learning Framework," IEEE Internet Things J., vol. 6, no. 1, pp. 124–135, 2019, doi: 10.1109/JIOT.2018.2872122.

[8] M. Jain and R. Saxena, "Overview of VANET: Requirements and its routing protocols," Proc. 2017 IEEE Int. Conf. Commun. Signal Process. ICCSP 2017, vol. 2018-Janua, pp. 1957–1961, 2018, doi: 10.1109/ICCSP.2017.8286742.

[9] K. Verma, H. Hasbullah, and A. Kumar, "Prevention of DoS attacks in VANET," Wirel. Pers. Commun., vol. 73, no. 1, pp. 95–126, 2013, doi: 10.1007/s11277-013-1161-5.

[10] I. Standard, "INTERNATIONAL STANDARD ISO / IEC / IEEE Telecommunications and information," vol. 2012, 2012.

[11] M. R. Ghori, A. S. Sadiq, and A. Ghani, "VANET Routing Protocols : Review , Implementation and Analysis VANET Routing Protocols : Review , Implementation and Analysis," 2018.

[12] P. Vijayakumar, M. Azees, A. Kannan, and L. Jegatha Deborah, "Dual Authentication and Key Management Techniques for Secure Data Transmission in Vehicular Ad Hoc Networks," IEEE Trans. Intell. Transp. Syst., vol. 17, no. 4, pp. 1015–1028, 2016, doi: 10.1109/TITS.2015.2492981.

[13] Y. L. Khaleel, M. A. Habeeb, and B. Rabab, "Emerging Trends in Applying Artificial Intelligence to Monkeypox Disease: A Bibliometric Analysis," Appl. Data Sci. Anal., vol. 2024, pp. 148–164, 2024, doi: 10.58496/ADSA/2024/012.

[14] A. S. Albahri et al., "A systematic review of trustworthy artificial intelligence applications in natural disasters," Comput. Electr. Eng., vol. 118, 2024, doi: 10.1016/j.compeleceng.2024.109409.

[15] A. S. Albahri, Y. L. Khaleel, and M. A. Habeeb, "The Considerations of Trustworthy AI Components in Generative AI; A Letter to Editor," Appl. Data Sci. Anal., vol. 2023, pp. 108–109, 2023, doi: 10.58496/adsa/2023/009.

[16] M. A. Habeeb, Y. L. Khaleel, and A. S. Albahri, "Toward Smart Bicycle Safety: Leveraging Machine Learning Models and Optimal Lighting Solutions," in Proceedings of the Third International Conference on Innovations in Computing Research (ICR'24), K. Daimi and A. Al Sadoon, Eds., Cham: Springer Nature Switzerland, 2024, pp. 120–131.

[17] A. H. Alamoodi, M. S. Al-Samarraay, O. S. Albahri, M. Deveci, A. S. Albahri, and S. Yussof, "Evaluation of energy economic optimization models using multi-criteria decision-making approach," Expert Syst. Appl., vol. 255, p. 124842, 2024, doi: 10.1016/j.eswa.2024.124842.

[18] O. S. Albahri et al., "Selection of smartphone-based mobile applications for obesity management using an interval neutrosophic vague decision-making framework," Eng. Appl. Artif. Intell., vol. 137, p. 109191, 2024, doi: https://doi.org/10.1016/j.engappai.2024.109191.

[19] A. H. Alamoodi et al., "Selection of electric bus models using 2-tuple linguistic T-spherical fuzzy-based decision-making model," Expert Syst. Appl., vol. 249, p. 123498, 2024, doi: https://doi.org/10.1016/j.eswa.2024.123498.

[20] I. M. Sharaf, O. S. Albahri, M. A. Alsalem, A. H. Alamoodi, and A. S. Albahri, "A novel dual-level multi-source information fusion approach for multicriteria decision making applications," Appl. Intell., vol. 54, no. 22, pp. 11577–11602, 2024, doi: 10.1007/s10489-024-05624-6.

[21] A. H. Alamoodi et al., "A Novel Evaluation Framework for Medical LLMs: Combining Fuzzy Logic and MCDM for Medical Relation and Clinical Concept Extraction," J. Med. Syst., vol. 48, no. 1, p. 81, 2024, doi: 10.1007/s10916-024-02090-y.

[22] S. Mishra and A. R. Tripathi, "AI business model: an integrative business approach," J. Innov. Entrep., vol. 10, no. 1, p. 18, 2021.

[23] R. Abduljabbar, H. Dia, S. Liyanage, and S. A. Bagloee, "Applications of artificial intelligence in transport: An overview," Sustainability, vol. 11, no. 1, p. 189, 2019.

[24] M. Coeckelbergh, "AI for climate: freedom, justice, and other ethical and political challenges," AI Ethics, vol. 1, no. 1, pp. 67–72, 2021.

[25] H. Ji, I. Han, and Y. Ko, "A systematic review of conversational AI in language education: Focusing on the collaboration with human teachers," J. Res. Technol. Educ., vol. 55, no. 1, pp. 48–63, 2023.

[26] F. K. H. Mihna, M. A. Habeeb, Y. L. Khaleel, Y. H. Ali, and L. A. E. Al-Saeedi, "Using Information Technology for Comprehensive Analysis and Prediction in Forensic Evidence," Mesopotamian J. CyberSecurity, vol. 4, no. 1, pp. 4–16, 2024, doi: 10.58496/MJCS/2024/002.

[27] Y. L. Khaleel, M. A. Habeeb, A. S. Albahri, T. Al-Quraishi, O. S. Albahri, and A. H. Alamoodi, "Network and cybersecurity applications of defense in adversarial attacks: A state-of-the-art using machine learning and deep learning methods," J. Intell. Syst., vol. 33, no. 1, 2024, doi: 10.1515/jisys-2024-0153.

[28] M. A. Habeeb, "Hate Speech Detection using Deep Learning Master thesis," University of Miskolc, 2021. [Online]. Available: http://midra.uni-miskolc.hu/document/40792/38399.pdf

[29] S. Dadvandipour and Y. L. Khaleel, "Application of deep learning algorithms detecting fake and correct textual or verbal news," Prod. Syst. Inf. Eng., vol. 10, no. 2, pp. 37–51, 2022, doi: 10.32968/psaie.2022.2.4.

[30] Y. L. Khaleel, "Fake News Detection Using Deep Learning," University of Miskolc, 2021. doi: http://dx.doi.org/10.13140/RG.2.2.31151.75689.

[31] L. Alzubaidi et al., "MEFF – A model ensemble feature fusion approach for tackling adversarial attacks in medical imaging," Intell. Syst. with Appl., vol. 22, 2024, doi: 10.1016/j.iswa.2024.200355.

[32] Y. L. Khaleel, H. M. Abdulfattah, and H. Alnabulsi, "Adversarial Attacks in Machine Learning: Key Insights and Defense Approaches," Appl. Data Sci. Anal., vol. 2024, pp. 121–147, 2024, doi: 10.58496/ADSA/2024/011.

[33] M. E. Alqaysi, A. S. Albahri, and R. A. Hamid, “Evaluation and benchmarking of hybrid machine learning models for autism spectrum disorder diagnosis using a 2-tuple linguistic neutrosophic fuzzy sets-based decision-making model,” Neural Comput. Appl., 2024, doi: 10.1007/s00521-024-09905-6.

[34] L. Alzubaidi et al., “Comprehensive review of deep learning in orthopaedics: Applications, challenges, trustworthiness, and fusion,” Artif. Intell. Med., vol. 155, p. 102935, 2024, doi: https://doi.org/10.1016/j.artmed.2024.102935.

[35] Z. T. Al-Qaysi et al., “A comprehensive review of deep learning power in steady-state visual evoked potentials,” Neural Comput. Appl., pp. 1–24, 2024.

[36] Z. T. Al-qaysi, A. S. Albahri, M. A. Ahmed, and M. M. Salih, “Dynamic decision-making framework for benchmarking brain–computer interface applications: a fuzzy-weighted zero-inconsistency method for consistent weights and VIKOR for stable rank,” Neural Comput. Appl., vol. 36, no. 17, pp. 10355–10378, 2024, doi: 10.1007/s00521-024-09605-1.

[37] G. G. Shayea et al., “Fuzzy Evaluation and Benchmarking Framework for Robust Machine Learning Model in Real-Time Autism Triage Applications,” Int. J. Comput. Intell. Syst., vol. 17, no. 1, 2024, doi: 10.1007/s44196-024-00543-3.

[38] A. A. Magabaleh, L. L. Ghraibeh, A. Y. Audeh, A. S. Albahri, M. Deveci, and J. Antucheviciene, “Systematic review of software engineering uses of multi-criteria decision-making methods: Trends, bibliographic analysis, challenges, recommendations, and future directions,” Appl. Soft Comput., vol. 163, p. 111859, 2024, doi: 10.1016/j.asoc.2024.111859.

[39] M. A. Alsalem et al., “Evaluation of trustworthy artificial intelligent healthcare applications using multi-criteria decision-making approach,” Expert Syst. Appl., vol. 246, p. 123066, 2024, doi: 10.1016/j.eswa.2023.123066.

[40] S. Khatri et al., “Machine learning models and techniques for VANET based traffic management: Implementation issues and challenges,” Peer-to-Peer Netw. Appl., vol. 14, no. 3, pp. 1778–1805, 2021, doi: 10.1007/s12083-020-00993-4.

[41] M. I. Jordan and T. M. Mitchell, “Machine learning: Trends, perspectives, and prospects,” Science (80-.)., vol. 349, no. 6245, pp. 255–260, 2015.

[42] et al., “Supervised Machine Learning Algorithms: Classification and Comparison,” Int. J. Comput. Trends Technol., vol. 48, no. 3, pp. 128–138, 2017, doi: 10.14445/22312803/ijctt-v48p126.

[43] K. Beyer, J. Goldstein, R. Ramakrishnan, and U. Shaft, “When Is ``Nearest Neighbor'' Meaningful?,” in Database Theory --- ICDT’99, C. Beeri and P. Buneman, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 1999, pp. 217–235.

[44] G. E. P. Box and G. C. Tiao, “Bayesian inference in statistical analysis,” Int. Stat. Rev., vol. 43, p. 242, 1973.

[45] A. M. . Hamad, “A Review on the Impact of Fly Ash on the Resistance of Ultra-High Performance Concrete to Acid and Sulfate Attacks”, ESTIDAMAA, vol. 2024, pp. 7–14, Feb. 2024, doi: 10.70470/ESTIDAMAA/2024/002.

[46] L. Hussain, “Fortifying AI Against Cyber Threats Advancing Resilient Systems to Combat Adversarial Attacks”, EDRAAK, vol. 2024, pp. 26–31, Mar. 2024, doi: 10.70470/EDRAAK/2024/004.

[47] C. Cortes and V. Vapnik, “Support-vector networks,” Mach. Learn., vol. 20, no. 3, pp. 273–297, 1995, doi: 10.1007/BF00994018.

[48] S. H. WALKER and D. B. DUNCAN, “Estimation of the probability of an event as a function of several independent variables,” Biometrika, vol. 54, no. 1–2, pp. 167–179, 1967, doi: 10.1093/biomet/54.1-2.167.

[49] D. Basak, S. Pal, and D. Patranabis, “Support Vector Regression,” Neural Inf. Process. – Lett. Rev., vol. 11, 2007.

[50] M. Wang and J. Zeng, “Hierarchical Clustering Nodes Collaborative Scheduling in Wireless Sensor Network,” IEEE Sens. J., vol. 22, no. 2, pp. 1786–1798, 2022, doi: 10.1109/JSEN.2021.3132504.

[51] K. Krishna and M. Narasimha Murty, “Genetic K-means algorithm,” IEEE Trans. Syst. Man, Cybern. Part B, vol. 29, no. 3, pp. 433–439, 1999, doi: 10.1109/3477.764879.

[52] H. Ji, O. Alfarraj, and A. Tolba, “Artificial Intelligence-Empowered Edge of Vehicles: Architecture, Enabling Technologies, and Applications,” IEEE Access, vol. 8, pp. 61020–61034, 2020, doi: 10.1109/ACCESS.2020.2983609.

[53] Y. Li, E. Schofield, and M. Gönen, “A tutorial on Dirichlet process mixture modeling,” J. Math. Psychol., vol. 91, pp. 128–144, 2019, doi: https://doi.org/10.1016/j.jmp.2019.04.004.

[54] S. Chen and Y. Zhu, “Subpattern-based principle component analysis,” Pattern Recognit., vol. 37, no. 5, pp. 1081–1083, 2004, doi: https://doi.org/10.1016/j.patcog.2003.09.004.

[55] H. M. S. SALEEH, H. Marouane, and A. Fakhfakh , Trans., “A Novel Deep Learning Approach for Detecting Types of Attacks in the NSL-KDD Dataset”, BJN, vol. 2024, pp. 171–181, Sep. 2024, doi: 10.58496/BJN/2024/017.

[56] M. Meilă and H. Zhang, “Manifold Learning: What, How, and Why,” Annu. Rev. Stat. Its Appl., vol. 11, no. Volume 11, 2024, pp. 393–417, 2024, doi: https://doi.org/10.1146/annurev-statistics-040522-115238.

[57] D.-C. Feng, Y.-P. Liang, X. Ren, and J. Li, “Random fields representation over manifolds via isometric feature mapping-based dimension reduction,” Comput. Civ. Infrastruct. Eng., vol. 37, no. 5, pp. 593–611, 2022, doi: https://doi.org/10.1111/mice.12752.

[58] H. Iima and Y. Kuroe, “Swarm reinforcement learning algorithms based on Sarsa method,” in 2008 SICE Annual Conference, 2008, pp. 2045–2049. doi: 10.1109/SICE.2008.4654998.

[59] D. Kosmanos, D. Karagiannis, A. Argyriou, S. Lalis, and L. Maglaras, “Rf jamming classification using relative speed estimation in vehicular wireless networks,” arXiv Prepr. arXiv1812.11886, 2018.

[60] S. Roselinmary, M. Maheshwari, and M. Thamaraiselvan, “Early detection of DOS attacks in VANET using Attacked Packet Detection Algorithm (APDA),” 2013 Int. Conf. Inf. Commun. Embed. Syst. ICICES 2013, pp. 237–240, 2013, doi: 10.1109/ICICES.2013.6508250.

[61] M. Jazzar and M. Hamad, “An Analysis Study of IoT and DoS Attack Perspective,” in Proceedings of International Conference on Intelligent Cyber-Physical Systems, B. Agarwal, A. Rahman, S. Patnaik, and R. C. Poonia, Eds., Singapore: Springer Nature Singapore, 2022, pp. 127–142.

[62] J. R. Douceur, “The Sybil Attack,” in Peer-to-Peer Systems, P. Druschel, F. Kaashoek, and A. Rowstron, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2002, pp. 251–260.

[63] S. Pavlitskaya, S. Ünver, and J. M. Zöllner, “Feasibility and Suppression of Adversarial Patch Attacks on End-to-End Vehicle Control,” in 2020 IEEE 23rd International Conference on Intelligent Transportation Systems (ITSC), 2020, pp. 1–8. doi: 10.1109/ITSC45102.2020.9294426.

[64] R. Elnaggar, R. Karri, and K. Chakrabarty, “Security against data-sniffing and alteration attacks in IJTAG,” IEEE Trans. Comput. Des. Integr. Circuits Syst., vol. 40, no. 7, pp. 1301–1314, 2020.

[65] S. Mishra, X. Li, A. Kuhnle, M. T. Thai, and J. Seo, “Rate alteration attacks in smart grid,” in 2015 IEEE Conference on Computer Communications (INFOCOM), IEEE, 2015, pp. 2353–2361.

[66] L. Alzubaidi et al., “Reliable deep learning framework for the ground penetrating radar data to locate the horizontal variation in levee soil compaction,” Eng. Appl. Artif. Intell., vol. 129, p. 107627, 2024, doi: 10.1016/j.engappai.2023.107627.

[67] R. Z. Homod et al., “Optimal shifting of peak load in smart buildings using multiagent deep clustering reinforcement learning in multi-tank chilled water systems,” J. Energy Storage, vol. 92, p. 112140, 2024, doi: https://doi.org/10.1016/j.est.2024.112140.

[68] L. Alzubaidi et al., “A survey on deep learning tools dealing with data scarcity: definitions, challenges, solutions, tips, and applications,” J. Big Data, vol. 10, no. 1, p. 46, 2023, doi: 10.1186/s40537-023-00727-2.

[69] H. Henderi, T. Wahyuningsih, and E. Rahwanto, “Comparison of Min-Max normalization and Z-Score Normalization in the K-nearest neighbor (kNN) Algorithm to Test the Accuracy of Types of Breast Cancer,” Int. J. Informatics Inf. Syst., vol. 4, no. 1, pp. 13–20, 2021.

[70] M.-I. Nicolae et al., “Adversarial Robustness Toolbox v1. 0.0,” arXiv Prepr. arXiv1807.01069, 2018.