XAI Based Technique for Detecting and Understanding Position Falsification Attacks in VANET

Mahesh Abburi *, Arunita Jaekel *

*University of Windsor, Windsor, ON, Canada

***Abstract*—Vehicular Ad-Hoc Networks (VANETs), an emerging technology for vehicle-to-vehicle communication, has brought about significant advancements in road safety and traffic management into modern Intelligent Transportation Systems (ITS). However, it has also introduced critical security concerns, particularly regarding the integrity of data exchanged among vehicles. In this paper, we propose a machine learning based approach to detect position falsification attacks in VANETs, where malicious entities broadcast fictitious location information to disrupt traffic flow and compromise road safety. A key focus of our approach is not only to develop robust detection models but also to integrate XAI to enhance the interpretability of the outcomes. The goal is to make the underlying decision-making processes transparent and understandable, fostering trust and facilitating more accessible validation by human experts.**

***Index Terms*—VANET, Explainabale AI (XAI), VeReMi Dataset, Basic Safety Message, Position falsification attack**

I. Introduction

Vehicular ad hoc network (VANET) [1] is an emerging technology in the Intelligent Transportation System (ITS) [2] that aims to make the transportation network more efficient, secure, and safe, by sharing relevant time-critical information with surrounding vehicles and infrastructure nodes. VANET supports two types of applications: safety applications and comfort applications. Examples of safety applications are blind spot warnings, emergency alerts, and lane change assistance; while comfort applications include weather information, advertisements, pricing, and details about the nearest gas stations or restaurants etc. In addition to vehicles, infrastructure nodes such roadside units (RSU), which facilitate communication between vehicles and other infrastructures, and Central Authority/ Authorization Party, providing services such as vehicle registration and key revocation in case of misbehavior [3] form part of the VANET architecture.

Each vehicle in the network is equipped with an On-Board Unit (OBU), which periodically transmits the vehicle's status to other nodes in the network. Such messages are called Basic Safety Messages (BSM) and contain the vehicle's kinematic and other information, such as position coordinates, vehicle speed, heading, brake status and transmission time. These messages are digitally signed using cryptographic techniques [4] and broadcast every 100ms via Dedicated Short Range Communication (DSRC) [5]. The integration of Vehicular Ad-Hoc Networks (VANETs) into modern transportation systems has revolutionized road safety and efficiency, facilitating the exchange of critical safety information among vehicles [6]. However, this integration also introduces security vulnerabilities, including various types of attacks such as denial of service (DoS), data replay and position falsification attacks [7], posing a grave risk to road safety and transportation efficiency [8].

In this paper, we focus specifically on the detection of *position falsification attacks* [9]. These attacks involve the manipulation of the vehicle's location information that is included in each BSM and are sent by malicious or compromised nodes, with valid credentials to participate in the network. So, traditional cryptographic techniques are often insufficient in detecting these attacks, as they primarily focus on external threats rather than insider attacks within VANETs. Therefore, there is a pressing need to develop advanced detection techniques capable of accurately identifying these attacks. Machine Learning (ML) presents a promising approach to address this challenge, and a number of ML-based techniques have been proposed in recent years [10], [11], [12]. Although existing research has made strides in detecting such attacks using ML algorithms, they typically fail to provide any insight into the decision-making process of the deployed

ISBN 978-3-903176-72-0 © 2025 IFIP

models. Consequently, there remains a critical gap in comprehending the decision-making process of these models.

Our proposed approach aims to develop a ML-based misbehavior detection system for VANET that also offers transparency in the decision making process, by integrating Explainable Artificial Intelligence (XAI) principles [13], [14], to enhance the interpretability and trustworthiness of the ML models. This transparency is crucial in the context of VANET security, where the consequences of false positives or negatives can have far-reaching implications on road safety and traffic management.

II. Related Work

VANET provides numerous services through wireless channels, which also makes it susceptible to security and privacy threats [15]. Machine Learning (ML) presents a promising approach that can leverage the vast amount of data generated within VANETs to detect anomalous behaviors indicative of attacks. By training ML models on labeled datasets or employing unsupervised learning techniques, researchers can extract meaningful patterns from the data and build robust detection systems capable of identifying position falsification attacks in real-time.

A. Overview of Machine Learning and XAI

Machine learning, a branch of Artificial Intelligence, empowers machines to execute specific tasks efficiently by leveraging statistical learning [16]. Its applications span various fields like healthcare, e-commerce, facial recognition, and email spam filtering. By identifying patterns in input data, machine learning algorithms make predictions, categorize information, and address real world challenges [17]. Within Vehicular Ad Hoc Networks (VANETs), superfised classification algorithms [18], a subset of ML, have been shown to be effective in detecting various types of attacks to improve the security of highly dynamic vehicular networks [19] and many different classification algorithms, such as K nearest neighbor (KNN), decision trees, random forest etc., have been proposed in the literature for VANET misbehavior detection.

As AI systems become increasingly complex, there is a growing need to understand the rationale behind their decisions, particularly in critical domains such as healthcare, finance, and autonomous systems. XAI addresses this need by providing human-understandable explanations for AI-driven predictions and recommendations, fostering trust, accountability, and regulatory compliance [14]. Techniques such as feature importance analysis, rule-based systems, interactive visualization tools and other specialized XAI approaches enable users to comprehend and scrutinize AI models' decision-making processes. XAI approaches can be model specific or model agnostic. Model-specific techniques are designed for specific types of machine learning models. For example, for decision trees, the tree structure can be visualized to understand how the model makes decisions. On the other hand, model-agnostic techniques can be applied to any type of machine learning model. Examples of model-agnostic approaches include feature importance analysis, identifying the most important features used by the model as well as LIME (Local Interpretable Model-agnostic Explanations) and SHAP (SHapley Additive Explanations).

LIME is an XAI method that can explain the predictions of any classification or regression by approximating it locally with an interpretable model [13], by creating a simpler, transparent model around a specific data point. This local model tries to mimic the complex model's behavior for that particular instance, revealing which features were most influential in the original model's prediction. LIME is model-agnostic, and can be applied to any model like neural networks, decision trees, and support vector machines. SHAP is another XAI technique, but unlike LIME, which focuses on explaining specific instances, SHAP tries to explain both global model behavior and local instance behavior [20]. The SHAP summary plot provides a detailed interpretation of feature contributions to the machine learning model's predictions by assigning each feature an importance value called SHAP value. Unlike the traditional feature importance, which simply ranks features, SHAP values are calculated by considering the average marginal contribution of a feature across all possible feature combinations, ensuring fair allocation of importance. In this paper, we focus on model-agnostic techniques such as LIME and SHAP to provide explanations of the decision-making of the black-box models.

B. Machine Learning based Misbehavior Detection in VANET

One of the first works that uses ML-based misbehavior detection in VANET is [10], which used an ensemble machine learning approach to detect various types of attacks. In [21], the authors examine the vulnerability of vehicular networks to attacks like DoS, Sybil, and false alerts. They also highlight the limitations of cryptographic methods in preventing insider attacks. In this work, Random

Forest and Decision Trees were shown to outperform other classifiers. For the remainder of this section, we will review different techniques for detecting of position *falsification attacks*, which is the focus of this paper. Khot et al. [22] proposed a machine learning framework to predict the vehicle's next position in the network. The authors compared predicted and actual values in the BSM and classified vehicles accordingly. If the position does not match the prediction, it is classified as an attacker vehicle. In [23], the authors proposed a machine learning framework for misbehavior detection using VeReMi dataset [9]. Six new features were created, consisting of plausibility checks and quatitative metrics to describe a vehicle's behavior in the network. In [24] a misbehavior detection model was developed for false alert verification and position falsification attacks. The receiver vehicle calculates changes in speed, position, distance and RSSI value compared to the sending vehicle. The dataset includes all of these values as features, which are then analyzed using machine learning algorithms. The work in [25] proposes a technique that combines information from two consecutive BSMs to improve detection rates for location spoofing. By leveraging consecutive BSM data, the authors were able to achieve high precision and recall for both binary and multiclass classification.

The primary objective of ML based techniques for detecting position falsification has been to improve detection accuracy. Consequently, the vast majority of papers in this area do not explicitly focus on understanding why specific predictions are made. In recent years, a few papers have started integrating XAI with misbehavior detection to gain deeper insights into model behavior. In [26], the authors developed a misbehavior detection model for position falsification attacks that integrated XAI into the machine learning model for better interpretation of the model. The study uses the VeReMi dataset and results show high accuracies with random forest and decision tree algorithms. The work in [27] explored the integration of XAI techniques like LIME and SHAP for explanations of the model's decision-making, using Burst-ADMA [28] dataset.

III. Proposed XAI integrated misbehavior detection (XIMD) approach

In VANET communication, vehicles transmit BSMs periodically into the network. Standard cryptographic methods can be used to authenticate the sender. But they cannot guarantee the correctness of the contents, if sent by an attacker with valid credentials. The proposed XAI Integrated Misbehavior Detection (XIMD) approach aims to detect position falsification attacks, using machine learning algorithms and integrating XAI techniques like LIME and SHAP for explainability. The goal is to provide some interpretable insights into the model's predictions, enhancing the understanding and trust in the system's output. The overall model training and detection process is carried out in three main phases: i) Data pre-processing, ii) classification and iii) XAI techniques.

A. Data pre-processing and feature selection

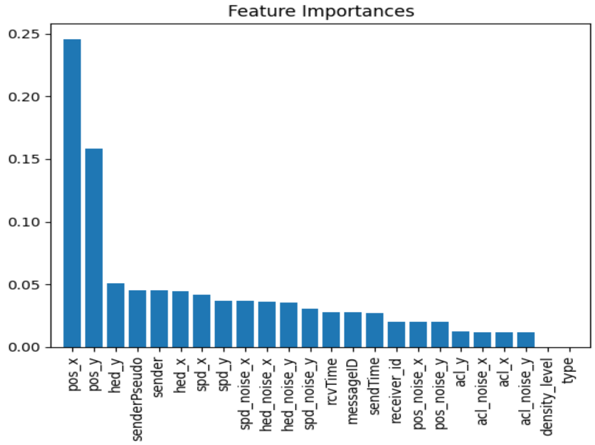

Fig. 1. Feature importance

The VeReMi dataset has a total of 225 simulations with different traffic scenarios, and each simulation consists of multiple log files (one for each vehicle) and a single ground truth file (with BSM information and identification of malicious vehicles). Each vehicle generates a log containing all received BSMs from other cars, including BSMs with false information received from malicious vehicles. Since the same BSM can be received by multiple vehicles, the merged log files have duplicate BSMs. The merged data is first pre-processed by removing any duplicates. Then information in the merged log file is combined with information from the ground truth file to identify malicious BSMs and generate a labeled dataset. Next, feature importance (FI) analysis is carried out and non-contributing features or feature with very low importance are filtered out.

Figure 1, shows the FI graph for constant position attack using random forest algorithm. From Figure 1, we can see that *position, heading*, and *speed* features contribute the most, while other features such as *acceleration* have relatively lower importance. Features such as *density_level* and *type* have no impact at all.

B. Classification

After data preprocessing and feature selection is completed, we split the data into a training set and a test set, with 80% of the data used for model training and the remainder for testing. In the VeReMi dataset, if a vehicle is an "attacker" then *all* its BSMs are labelled as malicious. So, if BSMs from the same sender appear in both the training and test sets, there is a high chance of overfitting. In this case, the model may simply memorize the identities of the attacker nodes instead of learning to detect suspicious patterns in the BSM data. Therefore, instead of randomly splitting the BSMs into training and test sets, we have implemented a customized algorithm that ensures that the two sets are *sender-disjoint*.

The VeReMi dataset contains five different types of position falsification attacks, as discussed below.

1) Constant Position Attack(CPA): The attacker continuously broadcasts the same position coordinates in each BSM.
2) Constant Position Offset Attack(CPOA): The attacker adds a constant offset to its actual position and transmits this altered position as part of the BSM.
3) Random Position Attack(RPA): The attacker inserts a random position coordinate in the BSM before sending.
4) Random Position Offset Attack(RPOA): The attacker inserts a random value from a preconfigured area around their vehicle in each BSM.
5) Eventual Stop Attack(ESA): The attacker behaves normally for some time and then suddenly sends a fixed position repeatedly.

In this stage, different ML algorithms are used to train the models with the training dataset. The models are trained on all five types of position falsification attacks mentioned above. We have used three supervised learning algorithms viz., Random Forest, Decision Tree and K-Nearest Neighbor (KNN) to train the models to classify received BSMs as legitimate or malicious.

C. XAI techniques

The final stage integrates XAI techniques like LIME (Local Interpretable Model-agnostic Explanations) and SHAP(SHapley Additive exPlanations) to create explanations for the black-box model's decision-making. LIME can reveal the original model's decision-making by assessing individual predictions to show how different features contribute to the decision-making of the model for a particular instance. Rather than focusing on a single prediction, SHAP values can be used to provide a better understanding of the feature importance for the entire dataset, indicating how much each feature's presence impacts the prediction. Examples of LIME and SHAP explanations for predictions of CPOA attacks is discussed in Sec. IV.B.

IV. Performance Evaluation

In this research, we use the VeReMi dataset [9], which uses Luxembourg traffic scenario(LuST) [29] and offers a wide range of different attack scenarios for evaluating the VANET misbehavior detection systems. Each prediction made by our proposed XIMD models falls in one of the following 4 categories:

- **True Positive(TP)** = instances correctly identified as positive(attacker)
- **True Negative(TN)** = instances correctly identified as negative(non-attacker)
- **False Positive(FP)** = instances incorrectly identified as positive(attacker)
- **False Negative(FN)** = instances incorrectly identified as negative(non-attacker)

To evaluate the performance of our proposed models, we use four key metrics: *Accuracy, Precision, Recall* and *F1-score* as defined below.

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN}$$

$$\text{Precision} = \frac{TP}{TP+FP}$$

$$\text{Recall} = \frac{TP}{TP+FN}$$

$$\text{F1-score} = 2 * \frac{Precision*Recall}{Precision+Recall}$$

The F1-score is a harmonic mean of precision and recall and can be a good indicator of overall performance, especially for unbalanced datasets.

A. Classification Results

Table I shows the classification results using different ML algorithms for each attack type. Random forest and decision tree models had very similar performances, with F1-scores of 90% or above for most attacks. RPOA was the hardest to detect for both models, with F1-scores of around 82%. KNN underperformed for all attack types, with significantly lower F1-scores, particular for RPOA.

TABLE I
Classification results of Proposed model

Algorithm	Acc.	Prec.	Recall	F1 Score
Constant Position Attack (CPA)				
Random Forest	92	92	91.25	89.71
Decision Tree	92.15	91.25	91.75	90.5
KNN	86.05	87.2	86.05	85.2
Constant Position Offset Attack (CPOA)				
Random Forest	92	92	92.25	92
Decision Tree	96	96	96	96
KNN	82	82	81	82
Random Position Attack (RPA)				
Random Forest	92.5	92.5	92.25	92.5
Decision Tree	92.7	92.4	91.75	91.9
KNN	89.05	89.2	89.05	89
Random Position Offset Attack (RPOA)				
Random Forest	82	82.6	82.25	81.71
Decision Tree	83.2	83.2	82.2	82.5
KNN	63.05	62.2	62.05	62.2
Eventual Stop Attack (ESA)				
Random Forest	92.5	92.6	92.5	92.4
Decision Tree	89.9	90	89.9	89.9
KNN	82.05	81.4	82.05	81.5

B. XAI Explanations

We have used LIME interpretations and SHAP values to understand the decision-making process for the above classification results. We have performed this analysis for all different attack types, with each of the 3 ML models (using random forest, decision tree and KNN). However, due to lack of space, we are including just one example of LIME and SHAP explanations using the *random forest* model for illustrative purposes. A more detailed analysis can be found in [30].

Figure 2 shows the LIME explanation for a constant position offset position falsification attack using random forest algorithm. The prediction probability of the top left portion of the image indicates the confidence of the model in its prediction. This particular example is a True Positive (TP), i.e., the BSM is malicious and identified as such, with a 91% confidence level. The center tree like structure highlights the contributions of various features to the prediction. Orange colour indicates the feature is contributing to classifying the BSM as malicious and blue as legitimate. Finally, the table on the right side shows each feature and its corresponding value for this particular instance. For this example, we see that the vehicle postion (pos_y(1138.18) & pos_x(1429.75)) and senderspeudo(106935) are the most impactful features and all three indicate the BSM should be classified as malicious. The remaining features have very little impact, with some indicating that it is malicious and others that it is legitimate. It is important to note that this LIME explanation is for this particular datapoint (BSM) only and each prediction will have its own corresponding explanation.

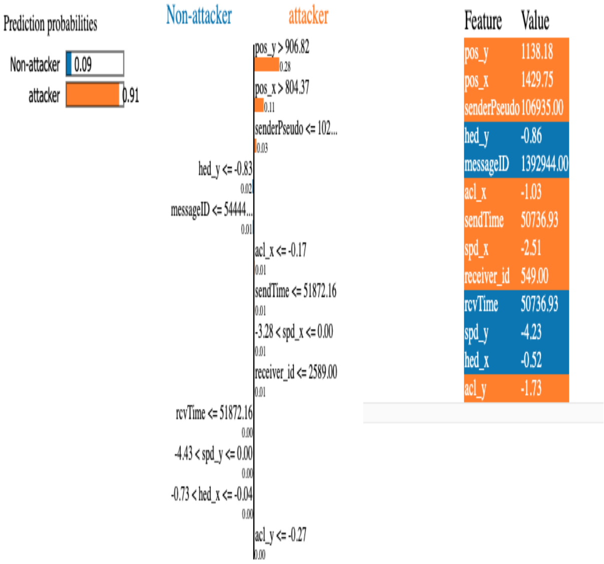

Fig. 2. Example of LIME Explanation

Figure 3 shows a summary plot of SHAP values for the constant position offset attack using random forest algorithm. This plot highlights pos_y, pos_x, and senderPseudo as the top 3 most influential features, with SHAP values indicating that higher values in these features significantly impact the model's outputs. The is in line with the top 3 features for the LIME example in Figure 2, although this may not always be the case. The heading(hed_y, hed_x) and speed(spd_y, spd_x) values also demonstrate some impact. In contrast, features such as rcvTime, sendTime, receiver_id and acceleration(acl_x, acl_y) exhibit minimal influence, as their SHAP values remain closely clustered around zero, indicating negligible contribution to the model's output. This analysis highlights the critical role of positional data in conjunction with other motion parameters such as speed and heading in identifying such attacks.

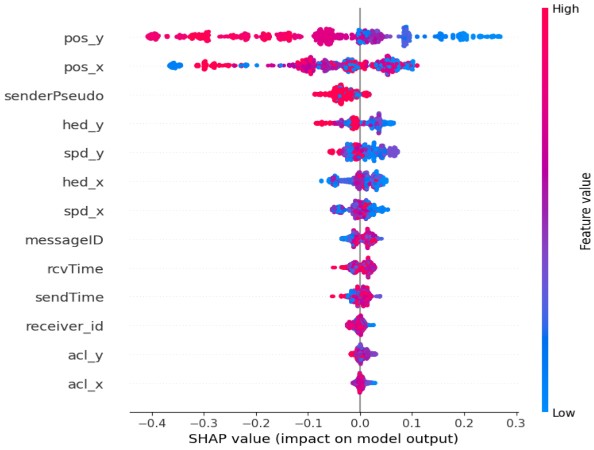

Fig. 3. Example of SHAP Explanation

C. Comparison with Existing Approaches

As mentioned previously, the vast majority of detection techniques for position falsification attacks do not consider XAI. The work in [27] does incorporate LIME and SHAP explanations, but uses the BurST-adma dataset instead of VeReMi. Therefore, we have compared our approach with the following two ML-based approaches:

- Paper1 [23]: uses plausibility checks and ML for misbehavior detection
- Paper2 [24]: uses different supervised ML models for misbehavior detection

Based on the performance of the different classifiers in our approach, we selected Random Forest with XAI model to compare with the existing techniques. We have selected F1-score as the comparison metric, as it incorporates both precision and recall and is a good indicator of overall performance. Table II shows a comparison of the F1-scores of the proposed XIMD technique with those in Paper1 and Paper2, for each of the five attack types.

TABLE II
Comparison of F1-scores with existing approaches

Approach	Attack Types				
	CPA	**CPOA**	**RPA**	**RPOA**	**ESA**
Paper1 [23]: ML (no XAI)	89	28	89	89	54
Paper2 [24]: ML (no XAI)	99.5	86	99.5	96	95
Proposed (XIMD): ML+XAI	90	92	92.5	82	92

Paper1 has the lowest performance for most attack types, particularly CPOA and (ESA). Paper 2 has F1-scores above 95% for most attacks and shows the best overall performance. The proposed approach results in F1-scores of 90% or higher for all attack types, except RPOA. Typically, its performance is close to, but slightly below that of Paper2. For CPOA, the proposed approach has the best performance, and is the only method with F1-score above 90%.

We note that when testing our models, we made sure that BSM senders in the training and test sets were *disjoint*. This is important, as having the same vehicle in both sets can lead to possible overfitting and skewing of test scores. Our proposed approach is capable of achieving similar performance, even compared to existing approaches that allow vehicle overlap between training and test sets.

V. Conclusion

Explainable AI (XAI) techniques are essential for improving transparency and building trust in predictions made by ML models. This is particularly important for intelligent transportation systems, where the decisions may have significant impact on both road safety and users. In this paper, we present a novel XAI integrated misbehavior detection (XIMD) approach for position falsification attacks in VANET. The proposed approach applies XAI techniques such as LIME and SHAP to provide explanations of the classifications made by our models. Unlike most existing approaches, we have implemented a custom *sender-disjoint* technique for creating the training and test sets, to avoid data leakage. Our models yield F1-scores of 90% or higher for most attack types, and compare favorably even with existing approaches that allow vehicle overlap. In future work, we plan to train our models to detect other attack types such as speed falsification, denial of service and data replay. We also plan to investigate the use of deep learning models to further improve the performance.

References

[1] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, "A comprehensive survey on vehicular ad hoc network," *J. of network and computer applications*, vol. 37, pp. 380–392, 2014.

[2] S.-h. An, B.-H. Lee, and D.-R. Shin, "A survey of intelligent transportation systems," in *2011 Third International Conference on Computational Intelligence, Communication Systems and Networks*. IEEE, 2011, pp. 332–337.

[3] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (vanets): status, results, and challenges," *Telecomm. Systems*, vol. 50, no. 4, pp. 217–241, 2012.

[4] S. S. Manvi and S. Tangade, "A survey on authentication schemes in vanets for secured communication," *Vehicular Communications*, vol. 9, pp. 19–30, 2017.

[5] J. B. Kenney, "Dedicated short-range communications (dsrc) standards in the united states," *Proceedings of the IEEE*, vol. 99, no. 7, pp. 1162–1182, 2011.

[6] M. Raya and J.-P. Hubaux, “Securing vehicular ad hoc networks,” *J. of computer security*, vol. 15, no. 1, pp. 39–68, 2007.

[7] I. A. Sumra, I. Ahmad, H. Hasbullah *et al.*, “Classes of attacks in vanet,” in *2011 Saudi Int. Electronics, Communications and Photonics Conf. (SIECPC)*. IEEE, 2011, pp. 1–5.

[8] M. S. Sheikh and J. Liang, “A comprehensive survey on vanet security services in traffic management system,” *Wireless Communications and Mobile Computing*, vol. 2019, 2019.

[9] R. W. van der Heijden, T. Lukaseder, and F. Kargl, “Veremi: A dataset for comparable evaluation of misbehavior detection in vanets,” in *International Conference on Security and Privacy in Communication Systems*. Springer, 2018, pp. 318–337.

[10] J. Grover, V. Laxmi, and M. S. Gaur, “Misbehavior detection based on ensemble learning in vanet,” in *International Conference on Advanced Computing, Networking and Security*. Springer, 2011, pp. 602–611.

[11] P. K. Singh, S. Gupta, R. Vashistha, S. K. Nandi, and S. Nandi, “Machine learning based approach to detect position falsification attack in vanets,” in *International Conference on Security & Privacy*. Springer, 2019, pp. 166–178.

[12] A. Sonker and R. Gupta, “A new procedure for misbehavior detection in vehicular ad-hoc networks using machine learning.” *International Journal of Electrical & Computer Engineering (2088-8708)*, vol. 11, no. 3, pp. 2535–2547, 2021.

[13] M. T. Ribeiro, S. Singh, and C. Guestrin, “”why should i trust you?”: Explaining the predictions of any classifier,” in *Proc. 22nd ACM SIGKDD Int. Conf. on Knowledge Discovery and Data Mining*, ser. KDD ’16. New York, NY, USA: Association for Computing Machinery, 2016, p. 1135–1144.

[14] G. P. Reddy and Y. V. P. Kumar, “Explainable ai (xai): Explained,” in *2023 IEEE Open Conference of Electrical, Electronic and Information Sciences (eStream)*, 2023, pp. 1–6.

[15] M. Arif, G. Wang, M. Z. A. Bhuiyan, T. Wang, and J. Chen, “A survey on security attacks in vanets: Communication, applications and challenges,” *Vehicular Communications*, vol. 19, p. 100179, 2019.

[16] M. Mohammed, M. B. Khan, and E. B. M. Bashier, *Machine learning: algorithms and applications*. Crc Press, 2016.

[17] V. Chaoji, R. Rastogi, and G. Roy, “Machine learning in the real world,” *Proceedings of the VLDB Endowment*, vol. 9, no. 13, pp. 1597–1600, 2016.

[18] P. C. Sen, M. Hajra, and M. Ghosh, “Supervised classification algorithms in machine learning: A survey and review,” in *Emerging technology in modelling and graphics*. Springer, 2020, pp. 99–111.

[19] L. Liang, H. Ye, and G. Y. Li, “Toward intelligent vehicular networks: A machine learning framework,” *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 124–135, 2018.

[20] S. M. Lundberg and S.-I. Lee, “A unified approach to interpreting model predictions,” *Advances in neural information processing systems*, vol. 30, 2017.

[21] A. N. Upadhyaya and J. Shah, “Attacks on vanet security,” *Int J Comp Eng Tech*, vol. 9, no. 1, pp. 8–19, 2018.

[22] A. Khot and M. Dave, “Position falsification misbehavior detection in vanets,” in *Mobile Radio Communications and 5G Networks*. Springer, 2020, pp. 487–499.

[23] S. So, P. Sharma, and J. Petit, “Integrating plausibility checks and machine learning for misbehavior detection in vanet,” in *2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA)*. IEEE, 2018, pp. 564–571.

[24] S. Gyawali and Y. Qian, “Misbehavior detection using machine learning in vehicular communication networks,” in *ICC 2019-2019 IEEE International Conference on Communications (ICC)*. IEEE, 2019, pp. 1–6.

[25] A. Sharma and A. Jaekel, “Machine learning based misbehaviour detection in vanet using consecutive bsm approach,” *IEEE Open J. of Vehicular Technology*, vol. 3, pp. 1–14, 2022.

[26] H. Mankodiya, M. S. Obaidat, R. Gupta, and S. Tanwar, “Xai-av: Explainable artificial intelligence for trust management in autonomous vehicles,” in *2021 Int. Conf. on Communications, Computing, Cybersecurity, and Informatics*, 2021, pp. 1–5.

[27] H. A. Idris, A. Ahmad, M. U. Diginsa, B. Aliyu, A. Muhammad, A. A. Yahaya, and S. U. Suleiman, “Explaining machine learning based speed anomaly detection system using explainable artificial intelligence.”

[28] M. A. Amanullah, M. Baruwal Chhetri, S. W. Loke, and R. Doss, “Burst-adma: Towards an australian dataset for misbehaviour detection in the internet of vehicles,” in *2022 IEEE PerCom Workshops*, 2022, pp. 624–629.

[29] L. Codecá, R. Frank, S. Faye, and T. Engel, “Luxembourg sumo traffic (lust) scenario: Traffic demand evaluation,” *IEEE Intelligent Transportation Systems Magazine*, vol. 9, no. 2, pp. 52–63, 2017.

[30] M. Abburi, “Detecting and understanding position falsification attacks using explainable artificial intelligence,” Master’s thesis, University of Windsor, Windsor, Canada, 2024.