International Journal of Engineering Research and Development
e- ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com
Volume 22, Issue 2 (February 2026), PP 102-110

Authentication Protocol for A Secured 5G Enabled Communication for Vehicular AD-HOC Networks

Kubiat Afangide[1], Akaninyene Obot[2], Kufre Udofia[3]

Abstract
Vehicular Ad-hoc Networks (VANETs) have become critical components of intelligent transportation systems, particularly with the advent of 5G technology. However, security challenges, especially authentication vulnerabilities and Rogue Base Station (RBS) attacks, pose significant threats to these networks. This study presents a novel Machine Learning (ML)-based authentication protocol for secured 5G-enabled vehicular communications. The proposed model integrates advanced ML techniques to detect and prevent RBS attacks while ensuring ultra-reliable lowlatency communication (URLLC). Using synthetic datasets with varying sizes (90LBS–18RBS to 1000LBS–180RBS) and window sizes (WS=3 to WS=10), the model achieved exceptional performance with 99.9999% accuracy for the largest dataset. The results demonstrate a True Negative Rate (TNR) of 98–100% for RBS detection and a minimal False Positive Rate (FPR) of approximately 1%. Performance comparisons with existing protocols show that the proposed scheme requires fewer message exchanges (5 total messages versus 9–16 for other protocols) and lower computational costs across all entities (UE, gNB, and AMF). The authentication protocol was formally verified using AVISPA, confirming its robustness against various security threats. This research advances the state-of-the-art in VANET security by bridging the gap between theoretical authentication protocols and practical ML-based implementations suitable for resource-constrained vehicular environments.
Keywords: *Vehicular Ad-hoc Networks; 5G Authentication; Machine Learning; Rogue Base Station Detection; URLLC; Network Security; V2X Communication.*

Date of Submission: 05-02-2026 Date of acceptance: 16-02-2026

I. Introduction

Vehicular communication is defined as communication between vehicles and has become increasingly critical in modern transportation systems [1]. The main objective of deploying Vehicular Ad-hoc Networks (VANETs) is to reduce the level of accidents and enhance passenger safety, particularly for drivers navigating in urban areas [2]. As vehicle populations increase daily, the rate of accidents also rises, making inter-vehicular communication essential. For example, if vehicle A is moving ahead of vehicle B and suddenly encounters an accident due to a thunderstorm, applying its brakes, the brake sensors and rain sensors of vehicle A automatically activate and transmit an alert message to other vehicles. Upon receiving this alert, vehicle B slows down, demonstrating the practical utility of inter-vehicular communication [3]. Vehicular networks are emerging as a key application scenario for fifth-generation (5G) mobile communication systems. In the next decade, autonomous vehicles will represent one of the main transmitters and receivers of 5G vehicular networks [4]. Compared with traditionally manned vehicles, autonomous vehicles are extremely dependent on ultra-reliable low-latency communication (URLLC) in 5G vehicular networks. Considering the URLLC requirement, a joint model of reliability and latency must be investigated for 5G autonomous vehicular networks. Moreover, developing a solution for improving both reliability and latency in 5G autonomous vehicular networks, i.e., implementing URLLC, is a considerable challenge [5]. 5G networks provide unprecedented levels of flexibility and adaptability that are necessary to support critical applications with stringent requirements in key vertical markets, including automotive and mobility. The advent of 5G technology has ushered in a new era of connectivity, enabling high-speed data transfer, low latency, and massive device connectivity [6]. In the context of vehicular communications, 5G facilitates Vehicle-to-Everything (V2X) communication, allowing vehicles to communicate with each other and their surroundings [7]. This connectivity enhances road safety, traffic efficiency, and the overall driving experience. However, the increased interconnectivity also presents significant security challenges, particularly concerning the authentication of vehicles and communications [8]. Authentication protocols are critical for establishing trust in vehicular networks. They ensure that only legitimate entities can access and interact within the network, protecting against malicious attacks such as spoofing and denial of service [9]. Research indicates that traditional authentication methods may not suffice in the dynamic and resource-constrained environments characteristic of vehicular networks [1]. The unique requirements of 5G, including ultra-reliable low-latency communications (URLLC) and Enhanced Mobile Broadband (eMBB), necessitate the development of robust authentication protocols tailored to these needs [10]. Existing studies highlight various approaches to enhancing

authentication mechanisms in vehicular networks. For instance, some propose using blockchain technology to create decentralized authentication processes, while others have explored lightweight cryptographic methods suitable for vehicular devices with limited computational power. Despite these advancements, significant gaps remain in understanding the performance implications of these protocols in real-world 5G environments. This research addresses the following critical problems: Insufficient security measures to protect against sophisticated cyber threats, particularly Rogue Base Station (RBS) attacks; High latency in authentication systems, which is unacceptable in time-sensitive vehicular environments; Limited consideration of processing power and battery life constraints of vehicular devices in many existing protocols; Scalability challenges as the number of connected vehicles increases exponentially and Lack of standardization leading to compatibility issues between different manufacturers and systems.

This research makes several significant contributions to the field of VANET security:

1. Introduction of Machine Learning (ML) for designing and evaluating a secured 5G authentication protocol for vehicular communications, combined with advanced optimization techniques and robust security features to enhance network accuracy, latency, reliability, security robustness, and overall performance.
2. Implementation of AVISPA for formal verification of security analysis and validation of the proposed scheme, providing rigorous security assurance.
3. Utilization of cryptographic algorithms such as hash functions, symmetric-key or asymmetric-key algorithms, and digital signature algorithms to achieve high security and mutual authentication, bridging a significant gap in current research and advancing knowledge in this emerging field.
4. Comprehensive security and performance analysis testing the security functions of the designed protocol and comparing its computational and communication costs with existing protocols, while verifying conformance to 5G network requirements using the Dolev‑Yao intruder model.

The remainder of this paper is organized as follows: Section 2 presents related work in IoV intrusion detection and feature selection methodologies; Section 3 describes the proposed TVC-BGWO framework; Section 4 presents comprehensive experimental results; Section 5 concludes the paper with key findings, and future research directions.

II. Review of Related Works

This section presents a comprehensive review of recent contributions in the area of authentication protocols, machine learning-based security mechanisms, and 5G-enabled vehicular communications. The review is organized thematically to provide a structured understanding of the current state of research and to identify gaps that this study aims to address. Patel et al. [11] investigated the use of multiple machine learning approaches for identifying and categorizing anomalous behaviors within Internet of Vehicles (IoV) environments. Their work focused on detecting various cyber threats, such as Denial of Service (DoS) and spoofing attacks targeting vehicular parameters including gas level, RPM, speed, steering angle, and wheel status. To improve transparency and user trust, Explainable Artificial Intelligence (XAI) techniques were incorporated into the modeling framework. The authors employed real-time sensor data and applied extensive preprocessing steps, including median-based imputation, categorical feature encoding, min–max normalization, class imbalance correction using SMOTE, and dimensionality reduction via Principal Component Analysis (PCA). Several classifiers—namely Random Forest, XGBoost, Support Vector Classifier, Decision Tree, and Logistic Regression—were evaluated. Experimental results indicated that Random Forest produced the most reliable performance across both binary and multi-class scenarios, closely followed by XGBoost, whereas SVC and Logistic Regression showed comparatively lower effectiveness.

Aloqaily et al. [12] presented a supervised learning-based intrusion detection framework aimed at safeguarding in-vehicle communication networks within Connected and Autonomous Vehicles (CAVs). Their objective was to accurately differentiate normal Controller Area Network (CAN) traffic from malicious messages. The study utilized the Car Hacking Dataset released by the Hacking and Countermeasures Research Laboratory, which contains over sixteen million CAN-bus records encompassing four distinct attack categories. Seven supervised algorithms were assessed, including Decision Tree, Random Forest, Naive Bayes, Logistic Regression, XGBoost, LightGBM, and Multi-layer Perceptron. Among these, Random Forest and LightGBM achieved the highest performance, each recording an accuracy of 99.9% with very low false alarm rates.

Zhang et al. [1] proposed a computationally efficient intrusion detection model designed for IoV systems by combining Gaussian Random Incremental PCA with an Optimal Weighted Extreme Learning Machine. The learning model was further optimized using Dynamic Inertia Weight Particle Swarm Optimization to enhance classification accuracy. Validation experiments conducted on NSL-KDD and CIC-IDS-2017 datasets produced accuracy values of 91.02% and 94.67%, respectively. Additionally, the framework retained more than 96% of the original data information while significantly reducing feature dimensionality and detection time. However, a key limitation of this work is its reliance on general intrusion datasets rather than datasets specifically tailored to vehicular environments.

Ahmed et al. [13] developed a robust machine learning-based IDS aimed at mitigating DoS and DDoS attacks in Vehicular Ad Hoc Networks (VANETs) and IoV infrastructures. Their approach integrates Random Projection and Randomized Matrix Factorization techniques to extract relevant features and reduce dimensional complexity. Using an application-layer DoS dataset, the Random Forest classifier achieved perfect detection for benign traffic and near-perfect performance for attack instances. The overall average accuracy of 98.7% exceeded that of many existing models, indicating strong potential for real-time deployment.

Li et al. [14] introduced an edge-centric detection scheme known as RTED-SD, specifically designed to identify Sybil-based DDoS attacks in IoV networks. The framework employs entropy-based measurements to capture traffic distribution patterns and detect abnormalities, alongside a Fast Quartile Deviation Check algorithm to recognize sudden deviations. To ensure fast response, optimized sliding windows and incremental entropy computation were adopted, resulting in constant-time complexity. Furthermore, the authors proposed a new metric termed Temporal False Omission Rate to evaluate detection timeliness.

Aslam et al. [15] proposed a deep learning-driven IDS for the Internet of Automobiles capable of discriminating between legitimate and malicious vehicular data streams. Their solution utilizes an autoencoder-assisted Deep Neural Network and was benchmarked against CNN, RNN, LSTM, and GRU architectures. The proposed model demonstrated superior performance, achieving 99.48% accuracy, 98% precision, 97% recall, and a 99% F1-score, thereby outperforming competing deep learning approaches.

Tiwari et al. [16] designed a lightweight Fine Tree-based intrusion detection model trained on a hybrid 5G-LENA IoV dataset generated through NS-3 and SUMO simulations. By incorporating hyperparameter optimization and post-pruning strategies, the model achieved near-perfect classification performance across all evaluation metrics. Despite these impressive results, the study primarily relies on simulated data and does not explore important practical aspects such as energy efficiency, latency, or cross-dataset validation, which may affect real-world applicability.

2.1 Research Gaps and Motivation

A thorough examination of existing studies highlights several unresolved issues in the domain of 5G-enabled vehicular communications and authentication protocols. Although previous works have proposed intrusion detection systems, blockchain-assisted authentication schemes, and lightweight cryptographic techniques to mitigate security threats, limited attention has been given to integrating machine learning-based rogue base station (RBS) detection directly into authentication mechanisms. Moreover, many existing approaches lack formal security verification and comprehensive evaluation under realistic vehicular communication environments. To address these shortcomings, this study proposes a comprehensive machine learning-driven authentication protocol for 5G-enabled VANETs that combines RBS detection with authentication procedures, incorporates formal verification, and evaluates performance under realistic simulation scenarios.

3 Methodology

3.1 Research Design

This study adopts a simulation-based experimental research design to develop and evaluate a machine learning-based authentication protocol for 5G-enabled VANETs. The overall framework consists of four major phases: (i) realistic RBS data generation through simulation, (ii) development and training of machine learning models, (iii) design and formal verification of the authentication protocol, and (iv) performance evaluation and comparative analysis. Both quantitative metrics (accuracy, precision, recall, F1-score, communication overhead, and computational cost) and qualitative analysis (verification of security properties) are employed to comprehensively assess the proposed approach.

3.2 Materials

The materials utilized in this research are categorized into software tools and hardware resources, as presented in Table 1.

Table 1: Software and Hardware Requirements

Category	Component	Specification
3*Software Tools	Simulation Environment	MATLAB R2021b, Python 3.8
	ML Framework	TensorFlow 2.x, Keras API
	Security Verification	AVISPA (OFMC, CL-AtSe)
4*Hardware	Processor	Intel Core i5-8250U @ 1.6 GHz
	Memory	16 GB DDR4 RAM
	Storage	64 GB SSD
	Operating System	Ubuntu 20.04 LTS / Windows 10 Pro

3.3 Development of Machine Learning-Based Model

This work extends an existing base model to incorporate realistic rogue base station behavior and enhances the handover process to identify and ignore base station signals exhibiting rogue characteristics [7]. The model focuses on autonomous detection of RBS using features such as GPS coordinates of the legitimate base station (LBS), received signal strength (RSS), and the location of the platoon leader. Since acquiring extensive real-world UE measurements is costly and time-consuming, a simulation-based approach is adopted to generate large-scale datasets representing diverse operational scenarios. The resulting synthetic datasets are suitable for training and evaluating machine learning models, as well as for studying handover behavior and prevention strategies against RBS attacks.

3.4 Simulation of Rogue Base Station

In the simulated scenario, an attacker deploys an RBS near a roadway to monitor transmissions from a legitimate base station. After gathering sufficient information, the RBS attempts to imitate the LBS and attracts user equipment (UE) by transmitting a stronger signal through increased power or a directional antenna [17]. When the received power at the platoon leader exceeds that of the LBS by more than 5 dB, the UE is likely to initiate a handover to the RBS, enabling the attacker to inject malicious commands [7].

Rather than assuming extremely high transmission power, this study models the RBS using a lower-power transmitter equipped with a narrow-beam directional antenna. Antenna gain is expressed as:

$$G = \frac{\text{Area of Sphere}}{\text{Area of Antenna Pattern}} \tag{1}$$

For a rectangular antenna pattern, the gain is computed as:

$$G = \frac{4\pi}{\sin\theta \sin\phi} = \frac{41253}{BW_\theta \times BW_\phi} \tag{2}$$

where BW_θ and BW_ϕ denote azimuth and elevation beamwidths in degrees, respectively. Equal horizontal and vertical beamwidths are assumed, allowing beamwidth to be derived from the specified antenna gain. This information, combined with RBS location, determines whether the UE lies within the RBS coverage area.

In 5G networks, handover decisions are based on Measurement Reports derived from Synchronization Signal Blocks (SSBs) containing the Master Information Block (MIB). Since these signals lack intrinsic protection, the serving base station may incorrectly initiate a handover toward an RBS. Therefore, an ML-based protection mechanism is required.

3.4.1 Rogue Base Station Attack Model

The RBS attack scenario demonstrates that if the RBS successfully forges the identification parameters of the LBS, such as its frequency, cell identifier, Mobile Country Code (MCC) and Mobile Network Code (MNC), it masquerades as the LBS with higher RSS and declares itself available for connection. The handover decision in 5G RAN is based on data in the Measurement Report, where the UE measures signal power of surrounding cells based on the Synchronisation Signal Block (SSB).

3.5 A Flexible Testbed

3.5.1 Simulation Setup

The experiment was conducted in MATLAB Version R2021b and installed on a quad-core Dell machine with an Intel Core i5-8250U CPU and 16 GB of RAM. The simulation focuses on developing a tool for the synthesis of realistic MR data including both LBS and RBS, with the ability to specify simulated RBS actors at varying positions to model various scenarios.

The simulation tool positions the RBS beam in various positions against a genuine base station to create challenging situations for the proposed detection method, generating signal profiles for the RBS in different positions relative to the peak received signal from a legitimate BS.

3.5.2 Simulation of Realistic RBS Signals

The simulation model enables rapid and effective generation of data for different scenarios where RBS elements are positioned in locations that can potentially interfere with a 5G network. Changing simulation parameters makes it possible to produce MR data for UE's in diverse and dynamic environments and develop strategies to prevent such attacks.

3.5.3 Produce Measurement Report

The UE measurement reports defined in 3GPP TR 38.331 provide information relevant for identifying RBS, including the cell's identity and RSS. The 3GPP specification provides for the Measurement Report as a component that stores the 6 strongest RSS values at any time. At each timestamp, the received signals from the six dominating BS in the vicinity of the platoon leader are computed.

3.5.4 Preprocessing Stage

The preprocessing stage takes as its input an MR data stream and produces an ML dataset as its output, which is then supplied to the ML model for decision making. The data is arranged with each BS on a separate line, consisting of an identifier (L for LBS, R for RBS) and first set of consecutive RSS readings for that BS in the MR. The number of RSS samples in each BS set is referred to as the width of the sample window.

3.5.5 Classification

During ML classification, a technique is performed to determine whether an observation fits into a certain category. The goal is to build a binary classifier that can accurately recognise a stream of incoming signal values as either from an authentic or a rogue BS. The classifier is trained by feeding it successive data streams, indicating for each whether the stream represents a legitimate or rogue BS.

An artificial neural network algorithm is implemented with a binary classification Multi-Layer Perceptron (MLP) using sequential API with the following architecture:

- Input neuron layers: one neuron per input feature
- First hidden layer: 30 neurons with ReLU activation function and 'he_normal' weight initialisation
- Second hidden layer: 20 neurons with tanh activation function
- Third hidden layer: 5 neurons with ReLU activation function
- Final layer with sigmoid activation function
- Optimizer: SGD (Stochastic Gradient Descent) with binary cross-entropy loss function

3.6 Dataset Description

A synthetic dataset of simulated RSS measurements was generated to evaluate the proposed ML-based authentication protocol for RBS detection in V2X networks. Three datasets with different scales were created:

- 90 LBS and 18 RBS (90LBS–18RBS)
- 500 LBS and 90 RBS (500LBS–90RBS)
- 1000 LBS and 180 RBS (1000LBS–180RBS)

Each dataset includes GPS coordinates, RSS values, timestamps, and binary class labels indicating legitimate or rogue base stations. Data were partitioned into training and testing sets using 70/30 and 80/20 ratios.

3.7 Performance Metrics

Classifier performance is evaluated using accuracy, recall, precision, F1-score, and specificity. Let TP, TN, FP, and FN denote true positives, true negatives, false positives, and false negatives, respectively. The metrics are defined as [5]

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \tag{3}$$

$$\text{Recall} = \frac{TP}{TP + FN} \tag{4}$$

$$\text{Precision} = \frac{TP}{TP + FP} \tag{5}$$

$$\text{F1-score} = \frac{2 \times (\text{Precision} \times \text{Recall})}{\text{Precision} + \text{Recall}} \tag{6}$$

$$\text{Specificity} = \frac{TN}{TN + FP} \tag{7}$$

3.8 Experimental Setup

The machine learning model is implemented in Python 3.8 using TensorFlow and Keras. A Multi-Layer Perceptron (MLP) architecture with multiple hidden layers and ReLU activation functions is adopted. Dropout regularization is applied to reduce overfitting. Binary cross-entropy is used as the loss function, and the Adam optimizer is employed for training. Window sizes ranging from 3 to 10 consecutive RSS measurements are evaluated. Training is performed for 20 epochs with a batch size of 32 and a validation split of 30%.

3.9 Formal Security Verification

Formal verification of the proposed authentication protocol is carried out using AVISPA. The protocol is specified in HLPSL and analyzed using OFMC and CL-AtSe back-ends. Verification is conducted under the Dolev–Yao adversary model to confirm properties such as mutual authentication, confidentiality, integrity, and resistance to replay attacks.

4 Results and Discussion

4.1 Results

This section presents the experimental results obtained from evaluating the proposed ML-based authentication protocol. The results are organized by performance metrics, including accuracy, precision, recall, F1-score, and computational efficiency measures.

4.1.1 Accuracy

As expected, accuracy rises as the volume of data considered increases. With 500 LBS and 90 RBS, a 70/30 split between training and testing data produces an accuracy result of 0.975 for WS=3. This measure improves to 0.987 with an 80/20 split between training and testing data shown by the dashed green line. For the larger dataset, accuracy increases even more, reaching 0.997 for the 500LBS-90RBS dataset and 0.99999 for 1000LBS-180RBS.

4.1.2 Precision, Recall and F1-Score

Similarly, the factors of precision, recall, and F1-score also increase with larger datasets and training data. The larger the window size, the more data are available to make accurate decisions.

The accuracy measure demonstrates that WS=3 is not sufficiently reliable. WS=5 is significantly more reliable, whereas WS=7 demonstrates improved performance with an accuracy of 0.995. However, WS=10 is the best option overall with accuracy = 0.99999 for the largest dataset.

Although larger window sizes increase precision, excessively large windows may hinder connection due to longer blocking time for a potential BS, which may introduce latency. WS=12 and WS=15 were explored but showed no better results than WS=10; therefore, the experiment stopped at WS=10. The results for precision, recall, and F1-score, which are 0.997, 0.998, and 1.0 respectively for the 90LBS-18RBS dataset, with further improvements for larger datasets. TNR (RBS detection probability) and TPR (LBS detection probability) are regarded as the primary performance statistics. However, FPR and FNR are also important in preventing detection of RBS as legitimate and legitimate BS as RBS.

Table 2: FPR and FNR for Different Datasets (70%-30% Split)

Dataset	FPR				FNR			
	WS=3	WS=5	WS=7	WS=10	WS=3	WS=5	WS=7	WS=10
90LBS–18RBS	0	0	0	0	0	0	0	0
500LBS–90RBS	1.03	1.03	1.03	1.03	0	0	0	0
1000LBS–180RBS	0	0	0	0	0	0	0	0

Binary cross-entropy loss is used as the loss function. Results indicate that window size has no noticeable impact on loss rate, while larger datasets achieve lower loss.

Table 3: TPR and TNR for Different Datasets (70%-30% Split)

Dataset	TPR				TNR			
	WS=3	WS=5	WS=7	WS=10	WS=3	WS=5	WS=7	WS=10
90LBS–18RBS	100	100	100	100	100	100	100	100
500LBS–90RBS	100	100	100	100	–	–	–	98.97
1000LBS–180RBS	100	100	100	100	100	100	100	100

4.1.3 Computational Cost

The proposed scheme was evaluated on a laptop running 64-bit Windows 10 operating system with Intel Core i7-6500U CPU at 2.50GHz and 8 GB RAM. The pairing-based cryptography (PBC) library was used for algebraic operations. Measured times included:

- Bilinear pairing operation: 3.79 ms
- ECC-based scalar multiplication: 0.68 ms
- ECC point addition: 0.486 ms
- Hashing operation: 0.0036 ms/Byte

According to the comparison, the computational performance of the proposed scheme is much better than other schemes. Therefore, the protocol brings significant improvement to be suitable for all handover scenarios in 5G Vehicular Communication networks. While there are safeguards built into the 5G wireless standard that protect user data and ensure privacy is maintained throughout the network, the identification of rogue agents in mobile networks remains one of the most serious concerns in user and network security, as recognized by the 3GPP Security Group.

RBS attacks have been highlighted as a significant risk, and this study demonstrates that an ML methodology is the most effective strategy for classifying BS data. RBS-MLP, an AI analyzer, has been designed and implemented based on realistic synthetic datasets. It is 3GPP compatible, applies ML to collected MR, and detects rogues intelligently.

The system can be integrated into the gNodeB of a 5G RAN to help stop attacks from hackers. The technique has been applied to an extensive collection of data using a vehicular scenario to identify inconveniences in the received signal level when an RBS utilizes the identity of an LBS. The results reveal that the ML methodology is 99.999% accurate in some cases and provides a new baseline method for RBS identification.The the performance of the 1000/180 dataset with WS=10. The largest dataset provides better training for the ML, and larger windows allow the detection to perform better. Varying these parameters resulted in a detection accuracy of 99.9999% for the 1000/180 dataset and WS=10.

5 Conclusion

The study focused on modeling and performance analysis of an authentication protocol for secured 5G enabled communication for vehicle Ad-hoc Networks (VANETs). Exploiting simulation data and advanced evaluation metrics, the research identified that while there are safeguards built into the 5G wireless standard that protect user data and ensure privacy is maintained throughout the network, the identification of rogue agents in mobile networks remains one of the most serious concerns in user and network security, as recognized by the 3GPP Security Group.RBS attacks have been highlighted as a significant risk, and this study demonstrates that an ML methodology is the most effective strategy for classifying BS data. RBS-MLP, an AI analyzer, has been designed and implemented based on realistic synthetic datasets. It is 3GPP compatible, applies ML to collected MR, and detects rogues intelligently.The study emphasized the robustness of WS=10 which is the best option overall with accuracy=0.99999 for the largest dataset in scenarios involving malicious Base stations. WS=12 and WS=15 were explored but showed no better results than WS=10. The factors of precision, F1-score, and recall were 0.997, 0.998, and 1.0 for the 90LBS-18RBS dataset, improving with larger extensive datasets.Comparatively, TNR (RBS detection probability) and TPR (LBS detection probability) are regarded as primary performance statistics. However, FPR and FNR are also important in avoiding

detecting RBS as legitimate and legitimate BS as RBS. These results underline the significance of hybrid models for ensuring secure, efficient, and scalable communication in VNETs, particularly in environments characterized by high mobility and unpredictable BSs behaviour. The Machine Learning protocol proposed in this study offers significant advancements in the accuracy, efficiency, reliability, and security of VANETs. The protocol maintained low routing overhead while achieving a high packet delivery fraction and minimal end-to-end delay, making it suitable for dynamic, resource-constrained environments. Its robustness against RBS established it as a viable solution for ensuring secure communication in 5G Enabled Vehicular Communication. It also outperformed selected contemporary protocols in handling complex routing challenges, particularly under high mobility and adversarial threats. This ML methodology addressed notable gaps in recent studies, including:

- Limited application of advanced ML techniques for real-time anomaly detection and adaptive authentication
- Insufficient analysis of the impact of dynamic network parameters on authentication protocol performance
- Lack of comprehensive mathematical models for analyzing the reliability and latency of ML-based authentication protocols in vehicular networks

These results emphasize the methodology's importance in advancing the state-of-the-art for security protocols in Vehicular Adhoc Networks (VNETs). Future work should focus on the following directions: Evaluation of SySUHA for the design and performance analysis of the scheme for Mobile Networks, empirical Performance Validation should be carried out by demonstrating Vehicular Communication's superior performance through comprehensive empirical comparisons with widely used protocols such as AODV, ZRP, and DSR, highlighting its efficiency and reliability.

References

[1] Hong Zhang and Xinxin Lu. Vehicle communication network in intelligent transportation system based on internet of things. *Computer Communications*, 160:799–806, 2020.

[2] Harshada Magar, Archana S Ubale, Nilakshee Rajule, RR Gupta, and Vineeta Philip. Case studies and real-world deployment examples of vanets (vehicular ad-hoc networks). In *Deep Learning Based Solutions for Vehicular Adhoc Networks*, pages 303–339. Springer, 2025.

[3] Xiang Cheng, Dongliang Duan, Shijian Gao, and Liuqing Yang. Integrated sensing and communications (isac) for vehicular communication networks (vcn). *IEEE Internet of Things Journal*, 9(23):23441–23451, 2022.

[4] Fowzia Sultana Sowdagar and Krishna Naik Karamtot. Simulation and analysis of 5g waveforms to reduce ber for vehicular communications. *Vehicular Communications*, 47:100777, 2024.

[5] Maraj Uddin Ahmed Siddiqui, Hanaa Abumarshoud, Lina Bariah, Sami Muhaidat, Muhammad Ali Imran, and Lina Mohjazi. Urllc in beyond 5g and 6g networks: An interference management perspective. *IEEe Access*, 11:54639–54663, 2023.

[6] Bhavik Patel, Vamsi Krishna Yarlagadda, Niravkumar Dhameliya, Kishore Mullangi, and Sai Charan Reddy Vennapusa. Advancements in 5g technology: Enhancing connectivity and performance in communication engineering. *Eng. Int*, 10(2):117–130, 2022.

[7] M Saedi, A Moore, P Perry, and C Luo. Rbs-mlp: A deep learning based rogue base station detection approach for 5g mobile networks. *IEEE Transactions on Vehicular Technology*, 2024.

[8] Paul Agbaje, Afia Anjum, Arkajyoti Mitra, Emmanuel Oseghale, Gedare Bloom, and Habeeb Olufowobi. Survey of interoperability challenges in the internet of vehicles. *IEEE Transactions on Intelligent Transportation Systems*, 23(12):22838–22861, 2022.

[9] Shi Dong, Huadong Su, Yuanjun Xia, Fei Zhu, Xinrong Hu, and Bangchao Wang. A comprehensive survey on authentication and attack detection schemes that threaten it in vehicular ad-hoc networks. *IEEE Transactions on Intelligent Transportation Systems*, 24(12):13573–13602, 2023.

[10] Seyed Salar Sefati and Simona Halunga. Ultra-reliability and low-latency communications on the internet of things based on 5g network: literature review, classification, and future research view. *Transactions on Emerging Telecommunications Technologies*, 34(6):e4770, 2023.

[11] Tanish Patel, Rutvij Jhaveri, Dhavalkumar Thakker, Sandeep Verma, and Palash Ingle. Enhancing cybersecurity in internet of vehicles: A machine learning approach with explainable ai for real-time threat detection. In *Proceedings of the 40th ACM/SIGAPP Symposium on Applied Computing*, pages 2024–2031, 2025.

[12] Ahmad Aloqaily, Emad E Abdallah, Hiba AbuZaid, Alaa E Abdallah, and Malak Al-hassan. Supervised machine learning for real-time intrusion attack detection in connected and autonomous vehicles: A security paradigm shift. In *Informatics*, volume 12, page 4. MDPI, 2025.

[13] Rana Hassam Ahmed, Majid Hussain, Hassan Abbas, Samraiz Zahid, and Muhammad Hannan Tariq. Enhancing autonomous vehicle security through advanced artificial intelligence techniques. *Journal of Computer Science and Electrical Engineering*, 6(4):1–6, 2024.

[14] Jiabin Li, Zhi Xue, Changlian Li, and Ming Liu. Rted-sd: A real-time edge detection scheme for sybil ddos in the internet of vehicles. *IEEE Access*, 9:11296–11305, 2021.

[15] Nida Aslam, Rizwan Ali Shah, Syed Ali Nawaz, and Mubasher H Malik. Securing the road: advancing cybersecurity in internet of vehicles with deep learning. *Journal of Computing & Biomedical Informatics*, 2024.

[16] Pradeep Kumar Tiwari, Shiv Prakash, Animesh Tripathi, Tiansheng Yang, Rajkumar Singh Rathore, Manish Aggarwal, and Narendra Kumar Shukla. A secure and robust machine learning model for intrusion detection in internet of vehicles. *IEEE Access*, 2025.

[17] Jianfei Sun, Junyi Tao, Hao Zhang, Yanan Zhao, Liming Nie, Xiaochun Cheng, and Tianwei Zhang. A tamper-resistant broadcasting scheme for secure communication in internet of autonomous vehicles. *IEEE Transactions on Intelligent Transportation Systems*, 25(3):2837–2846, 2023.