World Electric Vehicle Journal

Article

Optimized Feature Selection for DDoS Attack Recognition and Mitigation in SD-VANETs

Usman Tariq

Management Information System Department, College of Business Administration, Prince Sattam bin Abdulaziz University, Al-Kharj 16278, Saudi Arabia; u.tariq@psau.edu.sa; Tel.: +966-11-588-7080

Abstract: Vehicular Ad-Hoc Networks (VANETs) are pivotal to the advancement of intelligent transportation systems (ITS), enhancing safety and efficiency on the road through secure communication networks. However, the integrity of these systems is severely threatened by Distributed Denial-of-Service (DDoS) attacks, which can disrupt the transmission of safety-critical messages and put lives at risk. This research paper focuses on developing robust detection methods and countermeasures to mitigate the impact of DDoS attacks in VANETs. Utilizing a combination of statistical analysis and machine learning techniques (i.e., Autoencoder with Long Short-Term Memory (LSTM), and Clustering with Classification), the study introduces innovative approaches for real-time anomaly detection and system resilience enhancement. Emulation results confirm the effectiveness of the proposed methods in identifying and countering DDoS threats, significantly improving (i.e., 94 percent anomaly detection rate) the security posture of a high mobility-aware ad hoc network. This research not only contributes to the ongoing efforts to secure VANETs against DDoS attacks but also lays the groundwork for more resilient intelligent transportation systems architectures.

Keywords: Distributed Denial-of-Service (DDoS); network resilience; real-time cooperative communication; filtering mechanisms; trust management; traffic analysis; cooperative decentralized intrusion detection system (CD-IDS); permissioned blockchain; Software Defined Vehicular Ad-Hoc Networks (SD-VANETs)

check for updates

Citation: Tariq, U. Optimized Feature Selection for DDoS Attack Recognition and Mitigation in SD-VANETs. *World Electr. Veh. J.* **2024**, *15*, 395. https://doi.org/10.3390/wevj15090395

Academic Editor: Carolina Tripp-Barba

Received: 23 July 2024
Revised: 19 August 2024
Accepted: 26 August 2024
Published: 28 August 2024

1. Introduction

VANETs are a transformative advancement in the evolution of intelligent transportation systems which integrate vehicles equipped with advanced communication technologies. These networks provide significant improvements in traffic efficiency and transportation safety by enabling vehicles to exchange information about road conditions accidents and traffic congestion in real-time. The architecture of VANETs includes both vehicle-to-vehicle (V2V) [1] and vehicle-to-infrastructure (V2I) [2] communications forming a dynamic network where data about vehicle speed and location are shared continuously. However, the open nature of wireless communication in VANETs introduces several security vulnerabilities. The wireless medium is inherently susceptible to various security threats such as eavesdropping, unauthorized access, and data tampering. Given that the information often pertains to safety-critical functions, the need for robust security measures is paramount. The implications of security breaches go beyond mere data loss, affecting human lives and vehicle safety.

Security in VANETs revolves around core requirements including confidentiality, integrity, availability, and non-repudiation. Confidentiality ensures that sensitive information such as vehicle location and driver behavior is not accessible to unauthorized entities by rendering it unreadable and inaccessible to unauthorized entities during transmission and storage. Integrity protects against unauthorized data modification, ensuring that the information transmitted in the network remains accurate and reliable. Availability guarantees reliable access to network services and information which is vital for safety-critical applications. Non-repudiation prevents denial of wrongdoing by ensuring that the actions or communications by a party are unequivocally traceable to their originator. Table 1 categorizes various DDoS attack vectors to facilitate a comprehensive understanding of potential security vulnerabilities within VANET environments.

Table 1. Taxonomy of DDoS attacks in VANETs.

Protocol	Attacks	Attacks on	Vehicular Unit	Communication Technology	OSI Stack	Ease of Attack	Ref.
CAN	Masquerading, Denial of service, Bus-off, Message spoofing	Availability, Authenticity and identification, Integrity and data trust	Infotainment and telematics, OBD-II ports	DSRC/WAVE, Bluetooth	Network, Datalink	Moderate	[3]
LIN	Eavesdropping, Jamming, Message spoofing	Confidentiality, Authenticity and identification	USB ports, Electric vehicle charging	Wi-Fi/WiMAX, RFID	Physical, Datalink	High	[4]
FlexRay	Replay, Synchronization Disruption, Header collision	Integrity and data trust, Availability	Infotainment and telematics	Cellular, UWB	Transport, Network	Moderate	[5]
MOST	Traffic confidentiality, Traffic integrity attacks	Confidentiality, Integrity and data trust	Infotainment and telematics	ZigBee, Bluetooth	Application, Session	Low	[6]
Ethernet	Denial of service, Network access attacks	Availability, Non-repudiation/Ac	OBD-II ports	DSRC/WAVE, UWB	Network, Transport	Moderate	[7]
Wi-Fi	Jamming attack, Response collision	Availability, Integrity and data trust	USB ports, Electric vehicle charging	Wi-Fi/WiMAX, Bluetooth	Physical, Datalink	High	[8]
Cellular	Eavesdropping, Traffic confidentiality attacks	Confidentiality, Authenticity and identification	Infotainment and telematics	Cellular, RFID	Network, Session	Moderate	[9]
Bluetooth	Spoofing, Bluejacking	Authenticity and identification, Confidentiality	Remote Keyless Entry Systems	Bluetooth, Wi-Fi	Physical, Application	Low	[10]
DSRC/WAVE	Spoofing, Replay attack, Message falsification	Authenticity and identification, Integrity	V2V, V2I communication	DSRC/WAVE, ZigBee	Network, Transport	Moderate	[11]
RFID	Eavesdropping, Spoofing	Confidentiality, Authenticity and identification	Vehicle access, Cargo tracking	RFID, Cellular	Physical, Network	High	[12]
ZigBee	Traffic integrity attacks, Message injection	Integrity and data trust, non-repudiation	Sensor networks, Vehicle diagnostics	ZigBee, Bluetooth	Network, Application	Moderate	[13]
UWB	Jamming, Eavesdropping	Availability, Confidentiality	High-precision location systems	UWB, Wi-Fi	Physical, Datalink	High	[14]
5G	Man-in-the-middle, Identity spoofing	Authenticity and identification, non-repudiation	Connected vehicles, Smart Road infrastructure	5G, Cellular	Session, Transport	Moderate	[15]

This research paper addresses the critical security vulnerabilities in VANETs, focusing on a selection of technologies that hold the potential to enhance network security. These technologies include fog nodes, decentralized settings, blockchain technologies, and Software-Defined Networking (SDN). Each technology is evaluated for its ability to fortify the network against specific types of attacks such as, but not limited to, the following: GPS spoofing and gray-hole attacks among others. Thus, the main contributions of this research are outlined as follows:

(a) Investigation into a cooperative decentralized intrusion detection system (CD-IDS) that integrates fog computing and consortium permissioned blockchain technology to address cyber anomalies, including malicious communication traffic analysis, GPS and node identity spoofing, data forgery, denial-of-authentication and services, and routing disruption attacks.

(b) Enhancement of scalability and response times through the implementation of real-time anomaly detection with fog computing, enabling rapid data processing and reducing latency to effectively mitigate security threats (i.e., DoS and DDoS).

(c) Exploration of SD-VANETs to separate control and data layers, allowing for dynamic network reconfiguration and improved security management.

(d) Real-time assessment of the application of the Synthetic Minority Over-Sampling Technique (SMOTE) to address minority class imbalance in intrusion detection, thereby increasing the detection accuracy of rare malicious events.

(e) Implementation and analysis of novel Attribute-Based Broadcast Encryption (ABBE) for secure group communications to ensure that only authorized vehicles can access transmitted messages.

(f) Development and deployment of novel strategies for anonymous V2V communication to protect user privacy from tracking and profiling while maintaining network efficiency.

(g) Conducted an in-depth comparative analysis between centralized and decentralized security approaches to evaluate their strengths and weaknesses, including their implications for scalability, security, and privacy.

(h) Ultimately, a novel hybrid machine learning model, combining Autoencoder with LSTM and Clustering with Classification, was proposed and rigorously evaluated for intrusion detection. The results demonstrated that this approach not only surpassed traditional techniques in accuracy but also provided a promising solution for enhancing security in vehicular communications.

The research paper progresses seamlessly from the Literature Review Section, where an extensive analysis of the existing literature on DDoS attacks in VANETs is presented, to the Proposed Methodology Section, which outlines novel DDoS detection techniques and countermeasures tailored specifically for VANETs. This progression reflects a comprehensive understanding of the challenges and complexities inherent in securing VANETs against DDoS threats. Following the proposed methodology, the Experimental Setup and Assessment Outcome Section provides detailed insights into the experimental design and evaluation process, demonstrating the effectiveness of the proposed techniques through rigorous emulation. Subsequently, the Results and Discussion Section offers a thorough analysis of the experimental findings, highlighting key observations and insights derived from the evaluation. Finally, the Conclusion Section succinctly summarizes the main findings of the research paper, emphasizing the significance of robust DDoS detection and countermeasure strategies in ensuring the safety and reliability of VANETs, while also outlining potential areas for future research and development.

2. Literature Review

An application of VANET [16] defines its utilization scope spanning multiple purposes and classifications based on the nature of communication between entities such as vehicle-to-vehicle and vehicle-to-RSU (roadside units) communications. These applications are broadly categorized into four groups. *Safety applications* encompass services that enhance the safety of vehicles and passengers with features like collision detection systems, real-time traffic information, and congestion-free route discovery. *Comfort applications* focus on the entertainment aspects for drivers and passengers, offering audio and video playback and gaming alongside functionalities like electronic toll collection and simplified urban parking solutions through VANET communications. *Commercial applications* enable the downloading of personalized vehicle settings and provide security for rented vehicles alongside leveraging VANETs for targeted advertising aimed at drivers, highlighting nearby amenities such as restaurants and hotels. *Environmental applications* are instrumental in gathering sensor-driven environmental data beneficial for travelers, offering weather-related travel advisories and suggesting alternative routes in adverse weather conditions such as snow or storms.

In the context of Figure 1, we initiated the investigation with the primary motivation to furnish an updated summary of the state of the art in VANETs and to study the security challenges and potential solutions within this field. To our knowledge, many studies in the domain of VANET security focus on specific problems (such as the communication jitter function, delay, packet drop, throughput anomalies, etc.) and take the form of general surveys [4,5,15]. Yet, some foundational papers have also addressed security issues, notably the work/research by Saleem et al. [17] who explored the problem of potential adversary-instigated collusion among smart vehicles. Souissi and colleagues in their significant contributions discussed the classification of attacks and introduced the attacker model, highlighting novel attacks like the hidden vehicle tunnel wormhole and Bush Telegraph [18]. Their research also set forth essential requirements for securing message exchanges in vehicular networks and tackled the security issues in group communications.

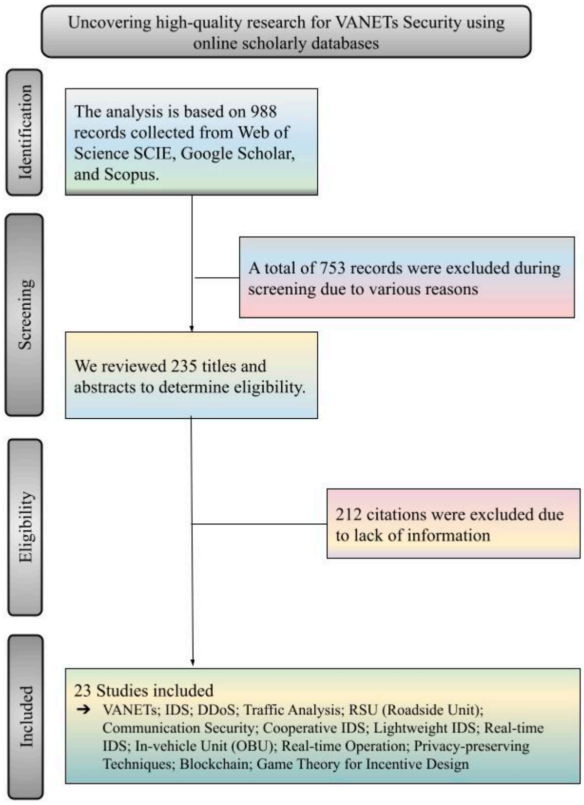

Uncovering high-quality research for VANETs Security using online scholarly databases
Identification
The analysis is based on 988 records collected from Web of Science SCIE, Google Scholar, and Scopus.
Screening
A total of 753 records were excluded during screening due to various reasons
We reviewed 235 titles and abstracts to determine eligibility.
Eligibility
212 citations were excluded due to lack of information
Included
23 Studies included
➔ VANETs; IDS; DDoS; Traffic Analysis; RSU (Roadside Unit); Communication Security; Cooperative IDS; Lightweight IDS; Real-time IDS; In-vehicle Unit (OBU); Real-time Operation; Privacy-preserving Techniques; Blockchain; Game Theory for Incentive Design

Figure 1. Visual illustration of the systematic search and screening strategy for literature review.

As a benchmark to this research evaluation, we aligned and applied the Smart Vehicle System Architecture (SVSA) as follows (i.e., partially illustrated in Figure 2) [1,3,6,8,11,13,17,18]:

(a) The core of the SVSA is the On-Board Unit (OBU), a powerful in-vehicle computer. The OBU typically utilizes a high-performance, low-power consumption automotive-grade processor like the NXP i.MX 8 series with real-time capabilities. This processor efficiently handles data collection, processing, and communication.

(b) The Vehicle Sensor Interface Module within the OBU connects to various sensors using CAN (Controller Area Network) bus for reliable in-vehicle communication. This module gathers data from GPS units with centimeter-level accuracy (e.g., u-blox NEO-M8N), high-resolution cameras (e.g., Sony IMX335), and radar sensors (e.g., Continental ARS4xx) for comprehensive situational awareness.

(c) For secure and reliable communication with other vehicles and RSUs, the OBU integrates a DSRC radio module compliant with the IEEE 802.11p standard. The DSRC radio typically operates in the 5.9 GHz band and offers high data rates (up to 6 Mbps) within a short range (typically 300 m).

(d) The inherent Security Module within the OBU safeguards communication by employing robust encryption algorithms like AES-128 and secure key management protocols like the DSRC Signed Message (DSM).

(e) A Trusted Platform Module (TPM) is often integrated to provide hardware-based security for cryptographic operations.

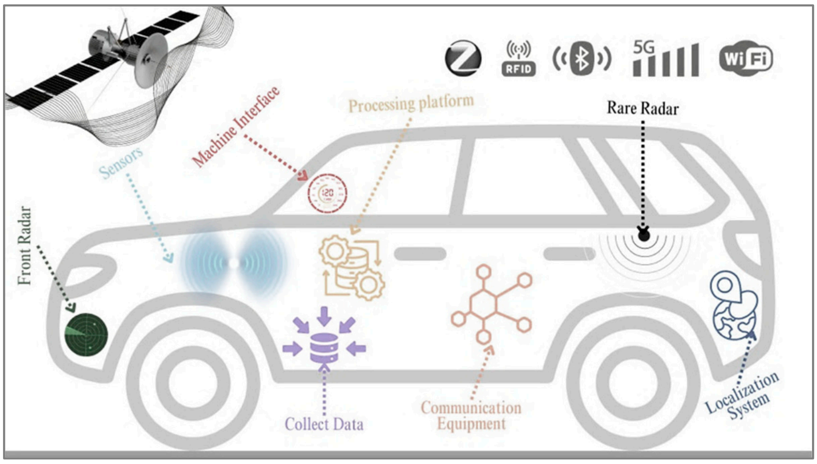


Figure 2. Advanced Smart Vehicle System Architecture in VANETs highlighting sensors, data processing, and connectivity technologies.

Table 2 presents the benchmarked specification of hardware components within the SVSA that were investigated for anomaly/exploits during DDoS attacks, for instance:

(a) Communication devices such as LTE and Wi-Fi modules are prone to flooding attacks [19] that might undermine the network's ability to relay crucial safety and operational data.

(b) Telematics control units essential for V2V and V2I communications could suffer from an overflow of malicious requests [20], potentially causing delays in vital information or spreading false data.

(c) Machine interfaces and external communication modules responsible for processing various sensor inputs and external data could be manipulated to produce false signals and data, resulting in system confusion and operational failures [21].

(d) Localization systems that rely on accurate GNSS timing signals can be disrupted, affecting the vehicle's navigation capabilities and possibly leading to safety risks on the road [22].

Table 2. Comprehensive hardware specifications for SVSA in V2V communication [1,3,6,8,11,13,17,18].

Component	Hardware Specification
Front Radar	**Model**: Bosch Mid-Range Radar Sensor MRR1PLUS; **Frequency**: 77 GHz; **Detection Range**: 160 m
Machine Interface	**Model**: NVIDIA DRIVE IX; **CPU**: 8-core ARMv8.2 64-bit CPU cores; **GPU**: Integrated 320-core Volta GPU; **Display**: Multi-modal input (touch, voice, gaze)
Communication Equipment	**Model**: Qualcomm Snapdragon X12 LTE; **Frequency Bands**: LTE FDD, LTE TDD (including CBRS support); **Wireless Standards**: 5G, 4G LTE, WCDMA, CDMA
Rare Radar	**Model**: Continental ARS408-21 Premium; **Frequency**: 77 GHz; **Detection Range**: 250 m; **Field of View**: Up to 120° horizontal
Localization System	**Model**: Trimble BX992 Dual Antenna GNSS; **Technology**: GPS, GLONASS, Galileo, BeiDou; **Accuracy**: Sub-meter to centimeter level
Sensors	**Model**: LIDAR-Lite v3HP; **Range**: 5 cm to 40 m; **Accuracy**: $+/-$ 2.5 cm; **Rate**: Up to 1 kHz
Processing Platform	**Model**: Intel Atom x7-Z8750; **Cores**: Quad-Core; **Frequency**: 1.6 GHz; RAM: 4 GB LPDDR3
Telematics Control Unit	**Model**: Autotalks CRATON2; **Communication**: DSRC/IEEE 802.11p, C-V2X; **Security**: Embedded HSM, Secure boot
On-Board Diagnostics (OBD) System	**Model**: ELM327 Bluetooth OBDII; **Protocols**: ISO15765-4 (CAN), ISO14230-4 (KWP2000), ISO9141-2, J1850 VPW, J1850 PWM
USB Ports	**Specification**: USB 3.1 Gen 1; **Data Transfer Rate**: Up to 5 Gbps
External Communication Module	**Model**: Sierra Wireless AirLink MP70; **Supports**: LTE-Advanced Pro, Wi-Fi, GNSS; **Designed for**: Vehicle networking
Infotainment System	**Processor**: Qualcomm Snapdragon 820Am; **Display**: 10-inch multi-touch screen; **Connectivity**: Bluetooth, Wi-Fi, USB
Vehicle Management System	**Model**: Bosch Vehicle Control Unit; **Functions**: Vehicle data monitoring, energy management, driver assistance systems
Energy Storage System	**Type**: Lithium-Ion Battery; Capacity: 100 kWh; **Features**: High voltage, fast charging capability

In consideration with Table 3, it is convincing to exhibit that DDoS attacks can cripple essential vehicular functions by targeting specific hardware such as front radars and communication equipment, leading to compromised safety and operational inefficiencies in V2V and V2I communications. By exploiting vulnerabilities in protocols like DSRC, GPS, and CAN, adversaries can also disrupt information flow, manipulate vehicle behaviors, and degrade the reliability and security of vehicular networks essential for dynamic and safe driving environments.

Table 4 categorizes security schemes based on attributes such as high mobility, flexibility, dynamism, link-ability, and traceability. It outlines two primary methods for data access: one depends on roadside infrastructure where vehicles connect via base stations like 5G, 4G LTE, WiMAX, or through access points like WiFi/802.11 and DSRC/802.11p, and the other employs direct vehicle-to-vehicle communications. The latter method enables vehicles to directly engage with nearby peers to exchange pertinent information independently of infrastructure, making it particularly advantageous and cost-efficient in rural or less urbanized regions. Our investigation has shown that reliance on cellular communications often presents limitations due to bandwidth constraints and the high costs associated with infrastructure development. In contrast, V2V communication stands out as a more adaptable and cost-effective option. The process of detecting mobility anomalies typically involves monitoring the distance between vehicles and flagging an anomaly when the distance exceeds a pre-established threshold. However, setting this threshold is challenging, especially when the vehicles being monitored are close to each other, as an excessively large threshold might not effectively detect anomalies. Various studies such as those by Su et al. [6], Pulligilla et al. [7], and others highlighted in the table show different levels of adherence to these attributes, reflecting the varied strategies employed to bolster security.

Table 3. DDoS attacks' impact on hardware components and targeted protocols [3–15].

Component	DDoS Attack Type	Impact	Impacted Hardware	Targeted Protocol
Vehicles	Vehicle-level jamming	Disruption of vehicle communications; safety risks	Front Radar, Communication Equipment	CAN, DSRC
Vehicles	GPS spoofing	Misguiding vehicles, leading to traffic inefficiencies	Localization System	GPS
Vehicles	Sybil attack	Creation of multiple fake identities to flood the network	Telematics Control Unit	DSRC, Cellular
Information	Bogus information dissemination	Spread of false information to overload network resources	Infotainment System	DSRC, Wi-Fi
Information	Message flooding	Overwhelming the network with excessive messages	Machine Interface	DSRC, LTE
Infrastructure	Infrastructure jamming	Disabling communication infrastructure	RSU Communication Equipment	DSRC, Cellular
Infrastructure	Network protocol attacks	Exploitation of protocol flaws to cause network outages	Network Processors	TCP/IP, DSRC
All Components	Malware propagation	Spreading malware across the network to create botnets	Entire Network System	All Vehicle Protocols

Table 4. Security systems' effectiveness and certificate cancellation patterns.

IDS Scheme	High Mobility	Flexibility	Dynamic	Link-Ability	Traceability
Su et al. [6]	✔	✖	✖	✔	✔
Pulligilla et al. [7]	✔	✖	✔	✖	✔
Xie et al. [9]	✔	✔	✔	✖	✖
Hosseinzadeh et al. [12]	✔	✖	✖	✔	✔
Saleem et al. [17]	✔	✖	✖	✔	✖
Shams et al. [20]	✔	✔	✔	✔	✔

3. Proposed Methodology

Our novel cooperative decentralized intrusion detection system (CD-IDS) integrates a hybrid detection technique by combining signature-based and anomaly-based methods. The traditional signature-based detection relies on known patterns of malicious behavior while anomaly-based detection assesses deviations from normal network operations. The dynamic nature of V2V and V2I communications can trigger a stealth pattern that has the capability of manipulating the traffic behavior to evade anomaly-based IDS. This pattern might involve (i.e., as illustrated in Figure 3), but is not limited to, the following:

(a) Crafting messages with characteristics that fall within the normal operating range but disrupt communication flow in a way that mimics background noise.

(b) Distributing a DDoS attack over a large number of compromised nodes, keeping individual attack traffic below anomaly thresholds. Unlike traditional networks with centralized control, VANETs rely on vehicle-to-vehicle communication, making it harder to pinpoint the source of an attack. The constant movement of vehicles creates a highly dynamic network topology, making it challenging to establish a baseline for normal traffic patterns.

(c) Injecting packets with forged source addresses to appear as legitimate network participants.

(d) Sending packets with random sizes to avoid triggering anomaly detection based on packet size patterns.
(e) Launching an anomaly in short bursts followed by dormant periods to mimic natural network traffic patterns.
(f) Disrupting network communication by manipulating routing protocols to create congestion or redirect traffic.

Herewith, Figure 3 effectively illustrates the sophisticated capabilities required by the anticipated 'anomaly detection engine' to proactively identify potential DDoS initiator anomalies. This engine necessitates to monitor a range of vehicle data, including speed for inconsistencies that might suggest spoofed locations or other deceptive practices, and GPS coordinates for sudden changes or improbable movements that could indicate location spoofing. It was also crucial to check the sequence and timing of messages with timestamps to pinpoint delayed or replayed traffic. By observing fluctuations in communication signal strength, the engine can detect variations that are atypical for standard vehicle movements or environmental conditions. Also, it aimed to evaluate traffic density data to identify potential flooding attacks and track erratic changes in vehicle acceleration that deviate from normal patterns. Monitoring brake status for unnatural patterns and detecting irregular steering behaviors are also essential for identifying compromised vehicle control systems. Proximity sensor readings help verify the actual proximity of vehicles, aiding in the detection of spoofed positions. Moreover, the engine may consider environmental conditions that could affect communication patterns and be exploited in sophisticated DDoS attacks. It is also prone to examine discrepancies in vehicle weight and load information, which could indicate false reporting or manipulation, and analyze diagnostic trouble codes to uncover signs of tampering or unusual error codes related to cyber-attacks.

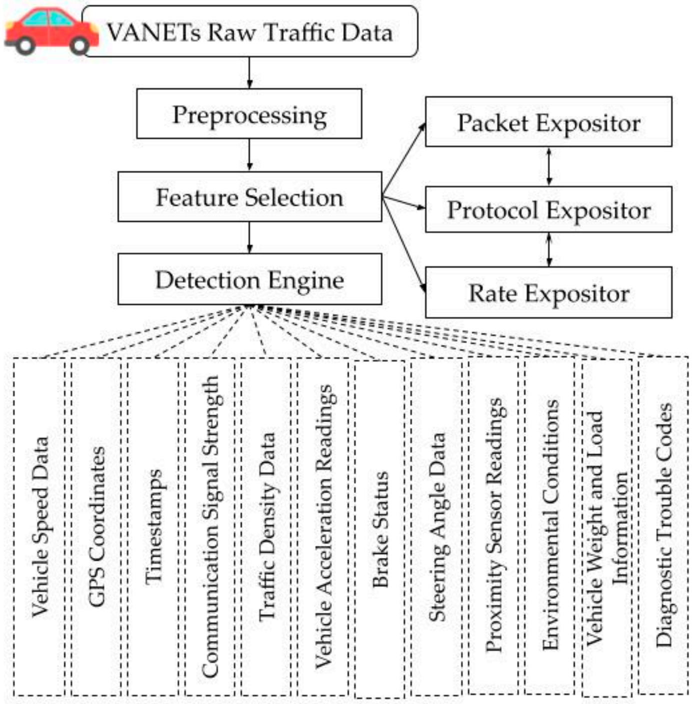


Figure 3. Detection of DDoS attacks based on anomalies.

Furthermore, in the proposed scenario, we envisioned that by blending malicious activity with legitimate traffic, the attacker aims to confuse the CD-IDS, making it difficult to distinguish the attack from regular fluctuations in network activity. Thus, we initiated the detection process with data aggregation where data from various sensors (i.e., identified in Table 2) and vehicles are collected. This was facilitated by the K-means clustering method (i.e., step-by-step processes are described in Algorithm 1 and Figure 4), which groups data from vehicles based on similarity metrics or by appointing certain vehicles as dedicated data collectors. The clustering is reflected in Equation (1):

$$J = \sum_{i=1}^{k} \sum_{x \in S_i} (x - \mu_i)^2 \tag{1}$$

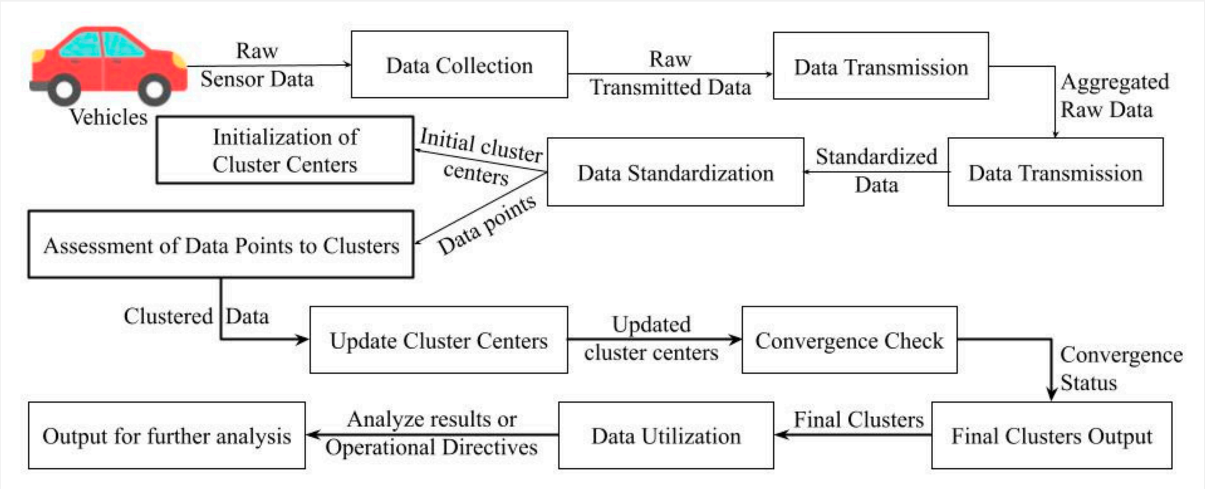


Figure 4. Step-by-step applied process of K-means clustering methodology.

In Equation (1), the J denotes the total within-cluster variance, k is the number of clusters, x represents data points in cluster S_i, and μ_i is the mean of points in S_i.

Algorithm 1. Applied K-means clustering method

Initialization	**Select** k initial cluster centers (means) randomly from the data points *(i.e., Vehicle speed data, GPS coordinates, Timestamps, Communication signal strength, Traffic density data, Vehicle acceleration readings, Brake status, Steering angle data, Proximity sensor readings, Environmental conditions (e.g., weather data), Vehicle weight and load information, Diagnostic trouble codes)*.
Assignment Step	**Assign** each data point to the cluster with the nearest center based on the distance between the point and each center.
Update Step	**Recalculate** the cluster centers as the mean of all points assigned to each cluster.
Convergence Check	**Determine** if the cluster assignments have changed from the previous iteration. If changes are minimal or none, proceed to termination; otherwise, repeat from the *Assignment Step*.
Termination	**Activate** Termination process when cluster centers stabilize with minimal or no change in assignments between successive iterations.

Following the aggregation of data, we implemented a filtering process using Principal Component Analysis (PCA), as detailed in Algorithm 2. This technique reduces the volume of data and improves the efficiency of the processing steps by eliminating redundant information. Redundant or irrelevant data were identified using the feature selection technique where only relevant attributes of data were kept for analysis:

$$F = \{f_1, f_2, \ldots, f_m\} \tag{2}$$

In Equation (2), F denotes the features selected from the total m features available within the dataset that has been gathered.

Algorithm 2. Applied Principal Component Analysis

Applied Steps	Processes
Data Standardization	Normalized the data points to have a mean of zero and a standard deviation of one for each feature in the dataset.
Covariance Matrix Computation	Calculated the covariance matrix to identify correlations between different features in the data. It involved the following steps: (a) Before calculating the covariance matrix, the proposed framework was mandated to standardize each feature in the aggregated dataset. This means subtracting the mean and dividing by the standard deviation for each feature, ensuring that all features contribute equally to the analysis. (b) Covariance was measured to determine if changes in one feature tend to be accompanied by changes in the same direction (positive covariance) or opposite direction (negative covariance) for the other feature, relative to their respective averages. The covariance matrix was calculated as follows: - Let matrix X capture the relationships between observations and features. Each feature is standardized and occupies a specific position within the matrix, allowing analysis of individual data points. - The covariance between two features i and j in the dataset was calculated as follows : $\sigma_{ij} = \frac{1}{n-1}\sum_{k=1}^{n} (x_{ki} - \mu_i)\left(x_{kj} - \mu_j\right)$ where x_{ki} and x_{kj} are the values of features i and j for observation k, and μ_i and μ_j are the means of features i and j, respectively. (c) A framework was coded to construct the Covariance Matrix as follows: - The covariance matrix Σ is an $n \times n$ symmetric matrix (where n is the number of features) with elements σ_{ij}. - The diagonal elements of the covariance matrix (where $i = j$) represent the variances of each feature, and the off-diagonal elements represent the covariances between pairs of features. (d) The matrix was formulated as follows: - The covariance matrix was implemented with dual functionality which could also be calculated in matrix form, and it was demonstrated to be more computationally efficient : $\Sigma = \frac{1}{n-1}\left(X^T X\right)$ where X is the matrix of standardized data (with each feature having zero mean), and X^T is the transpose of X.
Eigenvalue Decomposition	Computed the eigenvalues and eigenvectors of the covariance matrix to assess the principal components.
Principal Components Selection	Selected a subset of principal components that capture the most variance in the data while reducing dimensionality.
Data Transformation	Transformed the original data into a new subspace using the selected principal components to form the filtered dataset.

To create a real-time DDoS anomaly detection system powered by fog computing, we combined several cutting-edge techniques. These include fog computing itself, a weighted average method for gathering data efficiently, and a protocol for rapid information transfer within the fog layer (the complete framework architecture is detailed in Figure 5). Each of these techniques has been rigorously implemented, evaluated, and tested. The implementation of fog computing thresholds was key to determining significant anomalies. We defined a threshold function T that was based on the statistical variability in the data patterns, illustrated in Equation (3):

$$T(x) = \mu + \alpha \tag{3}$$

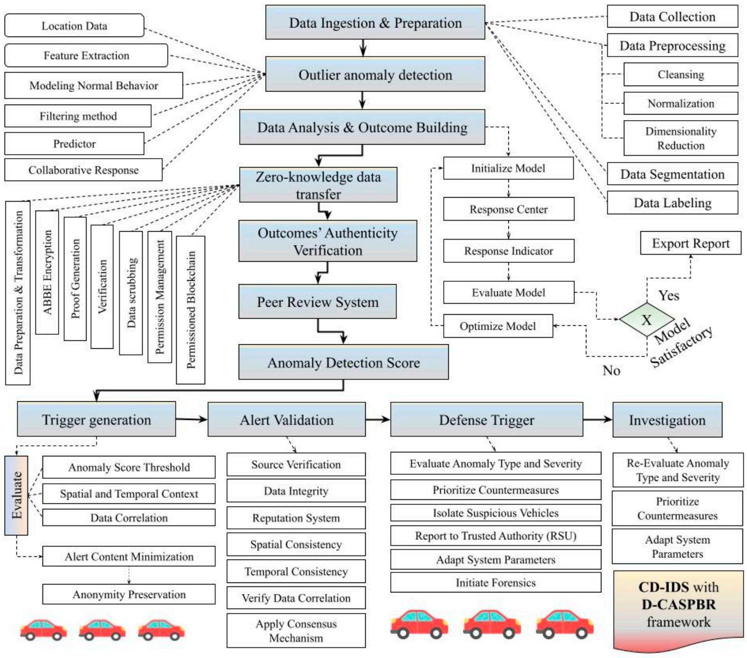


Figure 5. Framework architecture of novel cooperative decentralized intrusion detection system (CD-IDS) with Collaborative Anomaly Scoring and Permissioned Blockchain-Based Reputation (D-CASPBR).

Here, μ represents the mean of the observed data values, $x = \sigma$ is the standard deviation, and α is a scaling factor that adjusts the sensitivity of the detection process, ensuring that only significant deviations from the norm are reported. Following data aggregation (Figure 6), a standardization process was implemented to normalize the collected features. This ensured all features had equal weight during the analysis. This procedure involved adjusting each data point to zero mean and unit variance, effectively stabilizing variance across different types of vehicular data, which was critical for maintaining the integrity and comparability of subsequent analyses in our tested models.

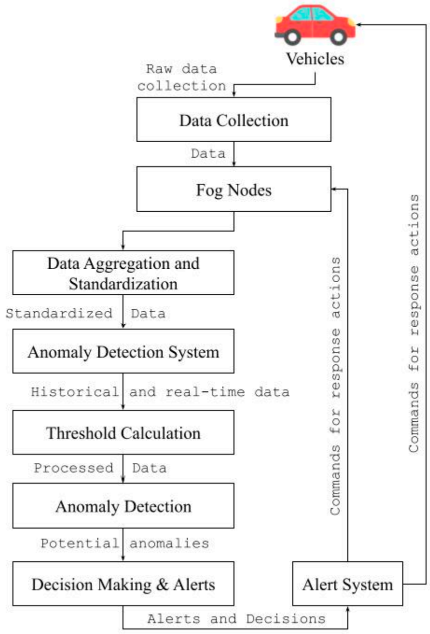


Figure 6. Implementation of fog computing thresholds determining significant DDoS anomalies.

For data aggregation, we employed a 'weighted average approach', allowing us to prioritize data based on their relevance and source reliability before aggregation. To estimate the weighted average, we employed parameters such as data freshness, source credibility, and contextual relevance to assign weights. These weights helped prioritize data based on their timeliness, reliability, and importance to the current analysis, ensuring the aggregated output was both accurate and reflective of the most pertinent information.

$$Aggregated\ result = \frac{\sum_{i=1}^{n} w_i x_i}{\sum_{i=1}^{n} w_i} \tag{4}$$

In Equation (4), x_i denotes the data value from vehicle i, w_i the weight assigned to this data point, and n the total number of data points, with weights assigned based on factors like timeliness, source credibility, or contextual relevance. Our choice of the real-time CD-IDS algorithm (i.e., exhibited in Figure 5) focused on leveraging machine learning techniques (i.e., *Autoencoder* with LSTM, and *Clustering* with *Classification*) that efficiently process and analyze vast data streams, maintaining high detection accuracy. Herewith (Equation (5)), we implemented the decision algorithm to trigger alerts based on the calculated probability $p(x)$ exceeding our defined threshold $T(x)$:

$$D(x) = \{_{0\quad otherwise}^{1\quad if\ p(x) \geq T(x)} \tag{5}$$

We also employed a novel system for communication protocols, including DSRC/IEEE 802.11p and C-V2X, as illustrated in Figure 7. This system was engineered to facilitate a swift information transfer, incorporating prioritization capabilities that distinguish between urgent and standard messages. This design was crucial for upholding network integrity and ensuring responsive communication across varied V2V and V2X conditions.

Herewith, to ensure data security, we implemented robust ABBE to safeguard communication between vehicles and fog nodes. The implemented method allowed the definition of access policies that dictate who can decrypt the transmitted messages based on their attributes, making it highly suitable for the V2X dynamic environment where vehicles might frequently join or leave the network. In the projected framework, the implementation of ABBE involved several key steps. First, the system defined a set of attributes relevant to the network participants, such as the vehicle type role in the network or geographical area. These attributes form the basis for policy definitions that control access to encrypted messages. When a message is sent, it is encrypted with a policy that specifies the suitable attributes that are required to decrypt it.

$$E_{\mathrm{ABBE}}(M, Policy) = Encrypt(M, K_{Policy}) \tag{6}$$

Here, in Equation (6), the M represents the message, *Policy* denotes the access policy, and K_{Policy} is a key derived from the attributes that satisfy the policy. The encryption function *Encrypt* takes the message and the policy key to produce the ciphertext. Decryption by a vehicle is only possible if it possesses a set of attributes that satisfies the policy associated with the ciphertext. The simplified decryption process is exhibited in Equation (7):

$$D_{\mathrm{ABBE}}(C, Attributes) = Decrypt(C, K_{Attributes}) \tag{7}$$

where C is the ciphertext, *Attributes* are the attributes held by the vehicle, and $K_{Attributes}$ is the decryption key derived from the vehicle's attributes. The function *Decrypt* uses the ciphertext and the decryption key to retrieve the original message if the 'attribute set' satisfies the policy. This attribute-based approach offered flexibility and enhanced security by ensuring that sensitive information is only accessible to vehicles with the correct credentials based on context-specific attributes rather than fixed identities. This method effectively prevents unauthorized access and ensures that even if a vehicle's network status changes, its ability to access new messages relies strictly on its current attributes aligning with the enforced policies.

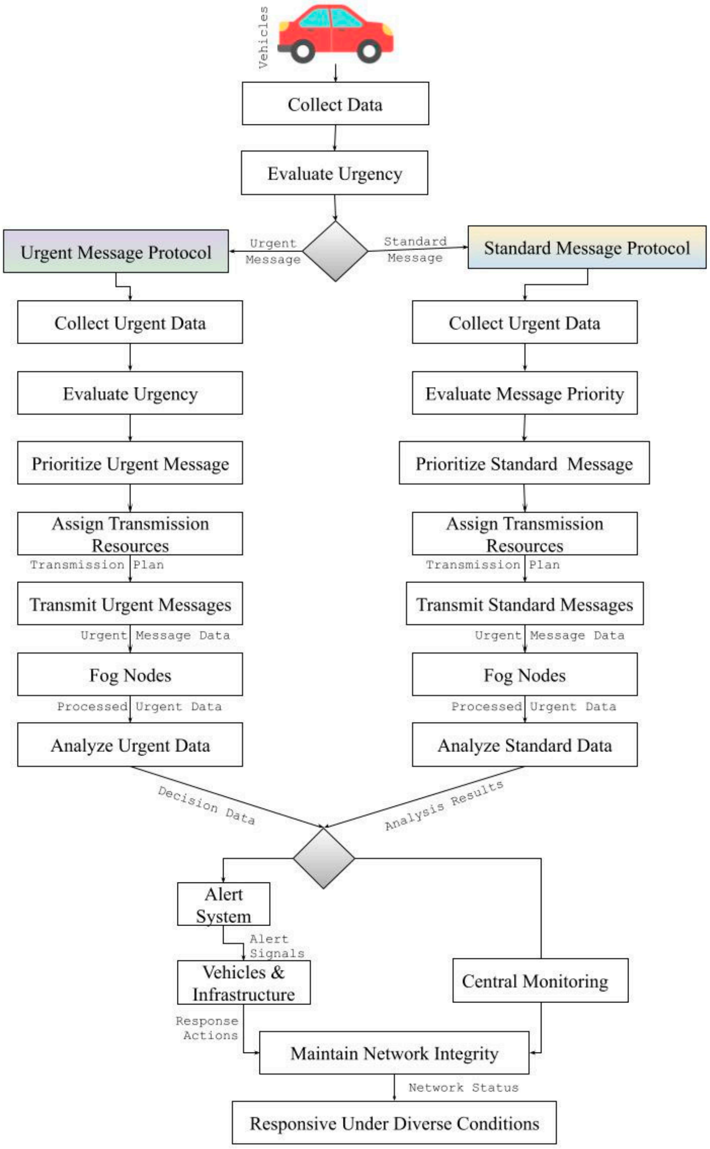


Figure 7. Rapid information transfer communication protocol.

During the deployment of ABBE, we optimized individual technical parameters to ensure robust and efficient performance. The encryption process used a 256-bit key size, conforming to high security standards suitable for protecting against sophisticated attacks (e.g., Sybil attack, spoofing attack, replay attack, Man-in-the-Middle Attack (MitM), etc.). The system was configured to execute encryption and decryption through a series of 12 rounds, which provided a comprehensive layer of security while balancing the computational load to avoid significant delays in communication. This configuration resulted in an average latency of approximately 5 ms per encrypted message, a minimal delay that is critical for maintaining real-time communication within VANETs. The processing size for each encryption or decryption operation is tightly controlled to accommodate the bandwidth constraints which are typical in vehicular networks, ensuring that the system can handle frequent and high-volume message exchanges without degradation of network performance.

We envisioned and exhibited that the effectiveness of ABBE in detecting and countering DDoS attacks lies in its attribute-based access control. This approach is particularly well-suited to dynamic network environments, where vehicles frequently enter and exit, ensuring robust security even in rapidly changing conditions. By requiring that each vehicle's attributes match specific criteria before decrypting received messages

$D_{\text{ABBE}}(C, Attributes) = Decrypt(C, K_{Attributes})$, ABBE effectively restricts access to network communications to authorized participants only. This attribute-based control mechanism significantly reduced the risk of DDoS attacks by limiting the ability of malicious entities to generate and disseminate high volumes of disruptive traffic. Vehicles without the necessary credentials were effectively barred from interacting with or disrupting the network, ensuring that potential threats were contained before they could cause widespread harm. This protection was crucial for maintaining continuous and secure vehicular communications.

To further enhance the network adaptability and security management, we integrated SD-VANETs. This implementation involved the critical separation of the control plane from the data plane, which allowed for centralized network management while maintaining the distributed nature of data forwarding. In our configuration, the SD-VANETs controller was tasked with managing the network's overall visibility, which included path configuration and traffic management. This centralized control proved essential for orchestrating coordinated responses to DDoS attacks, enabling the rapid identification and isolation of malicious traffic and nodes. The optimal routing decision within these SD-VANETs is illustrated in Equation (8):

$$R(s, d) = \min_{\forall p \in P_{s,d}} Cost(p) \tag{8}$$

where $R(s, d)$ indicated the optimal route from source s to destination d, $P_{s,d}$ denoted all possible paths, and $Cost(p)$ represented the cost function of each path. The dynamic reconfiguration of network routes was also a pivotal feature, allowing the network to adapt to varying conditions and threats dynamically. Traffic was rerouted away from congested or compromised nodes, effectively minimizing the impact of ongoing DDoS attacks. This dynamic route adaptation is captured by Equation (9):

$$R_{\text{new}}(s, d) = \min_{\forall p \in P_{s,d}} (Cost(p) + \Delta Cost(p, t)) \tag{9}$$

where in Equation (9), the $\Delta Cost(p, t)$ reflected changes in the cost function due to factors like network congestion or security breaches. Moreover, flow-based rules (i.e., block/forward) were applied to either block or safely redirect suspicious data flows, thereby preventing further network disruption. These security actions were governed by the following:

$$F(x) = \begin{cases} block & if \quad x \in X_{mal} \\ forward & otherwise \end{cases} \tag{10}$$

As demonstrated in Equation (10), $F(x)$ could determine the treatment of packet x, with X_{mal} being the set of data flows identified as malicious. Through the implemented SD-VANETs framework, the projected system was able to achieve improved traffic management, reduced communication overhead, and enhanced scalability to support a large and dynamically changing array of network nodes.

We also integrated permissioned blockchain that allowed only verified entities (i.e., V2V, V2X) to participate in the network, significantly reducing the risk of malicious activities and unauthorized data breaches. Each transaction or data exchange within the network was securely logged and immutable, providing a trustworthy and tamper-proof system. This was critical for maintaining a reliable audit trail and enforced the accountability that is vital in the dynamic environment of VANETs, where network nodes frequently change. We combined fog computing with permissioned blockchain to enhance the effectiveness of our CD-IDS. Fog computing enabled the local processing of data at the network's edge, which enabled the system to significantly reduce latency and also allowed for near real-time detection of anomalies. The integration process involved the deployment of fog nodes capable of executing local data analytics to swiftly detect potential anomaly activities:

$$F_{\text{local}}(v) = \sum_{i=1}^{n} a_i(v) \tag{11}$$

Here, as per Equation (11), F_{local} denotes the local processing function at fog nodes, v represents a vehicle, and $a_i(v)$ are the analytics operations performed on the data collected from vehicle v. Instantaneously, permissioned blockchain swiftly ensured that all communications between the fog nodes and vehicles were securely encrypted, which made the network accessible only to those with proper authorization credentials. The system employed the Elliptic Curve Digital Signature Algorithm (ECDSA), which is a well-established protocol for node authentication that aided in verifying vehicles to maintain a secure environment. Furthermore, the Practical Byzantine Fault Tolerance (PBFT) consensus mechanism within the blockchain was crucial in maintaining network integrity and availability, even amidst challenging scenarios like Sybil attacks, Byzantine failures, and collusion attempts. To bolster security further, smart contracts were integrated to enforce policies and swiftly respond to suspicious activities, consequently minimizing the impact of any attempted attacks on the network's operational capacity.

We addressed the minority class imbalance by employing the SMOTE [23]. This method helped in artificially generating new instances of the minority class, thus balancing the dataset and improving the detection accuracy for rare malicious events:

$$S_{\text{synthetic}} = S + \lambda(S_{\text{nn}} - S) \tag{12}$$

where in Equation (12), the S represents an original sample from the minority class, S_{nn} is its nearest neighbor in the feature space, and λ is a random number between 0 and 1. At this stage, we conducted a comparative analysis of a centralized and decentralized security approach. We evaluated their strengths and weaknesses, with findings indicating that while centralized systems offered easier management and implementation of security policies, decentralized systems provided better resilience against DDoS attacks and were more scalable.

In the final phase of our research, we successfully employed and evaluated a novel hybrid machine learning model. By integrating an Autoencoder with LSTM and combining it with the Clustering and Classification technique, we effectively harnessed the capabilities of both methods to identify complex DDoS patterns.

$$M_{\text{hybrid}} = \text{Autoencoder}_{\text{LSTM}}(\text{Cluster}(X)) \tag{13}$$

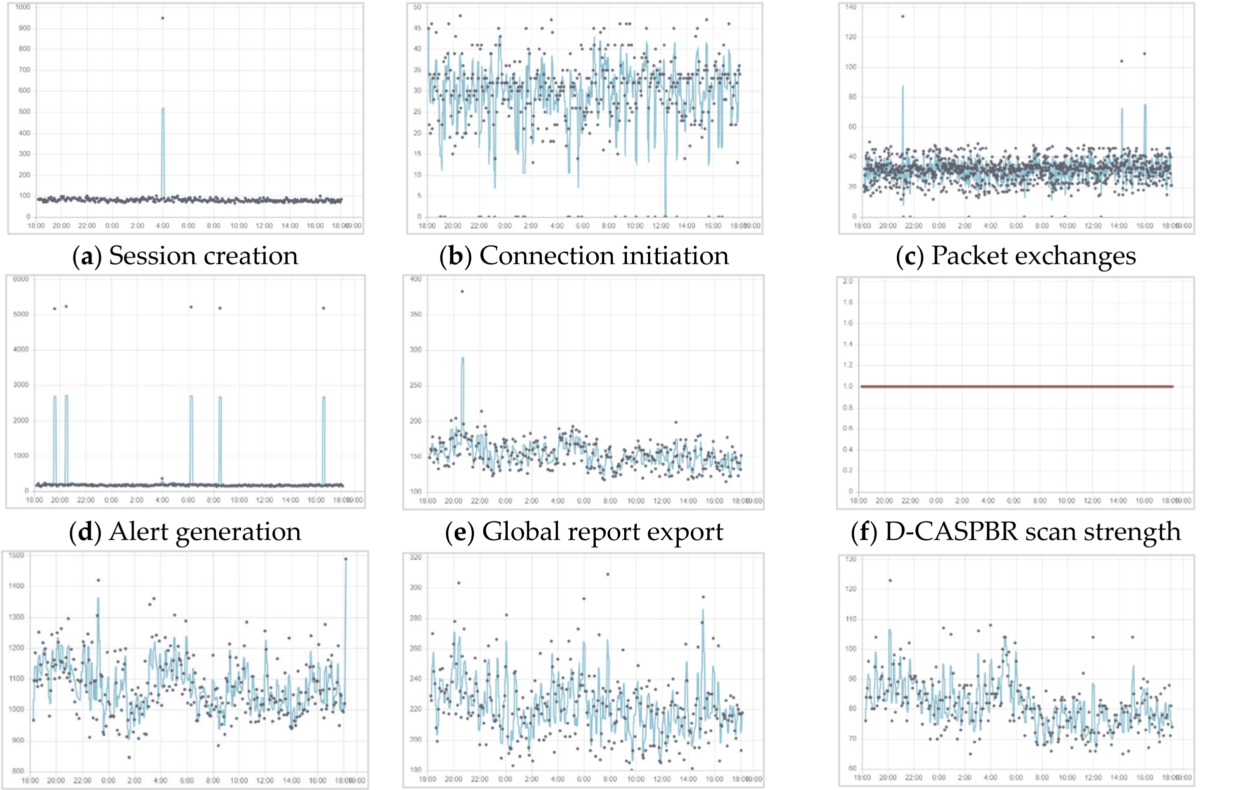
where M_{hybrid} represents the hybrid ML model, X is the input data set, and $\text{Cluster}(X)$ denotes the initial data clustering phase feeding into the LSTM-based Autoencoder. The hybrid model described by Equation (13), which incorporated an Autoencoder with LSTM, was specifically designed to process temporal sequences which are crucial for recognizing evolving malicious anomaly patterns. The architecture included two LSTM layers, each equipped with 128 units capable of capturing time-dependent features from network traffic data. The dimensionality of the data was significantly reduced through a bottleneck layer, which helped isolate crucial features by compressing the input into a more condensed format (i.e., latent space embeddings). This process was essential for focusing on the most important aspects of the data. Prior to the LSTM setup, K-means clustering, as depicted in Figure 4, segmented the input data into distinct clusters, thereby facilitating the classification process by grouping similar data points. The classification phase featured a dense layer with a softmax activation function tasked with categorizing the LSTM outputs into specific categories that represent various DDoS attack vectors. The optimization of this model was achieved using a learning rate of 0.001 and a dropout rate of 0.5 to bolster model generalization and avert overfitting during the training process. The model was subjected to extensive training and testing, proving its high accuracy and robustness in the detection and classification of DDoS threats.

4. Experimental Setup and Assessment Outcome

The OMNeT++ 6.0.3 simulator [24], coupled with a VANET infrastructure, was utilized to collect empirical data through a series of tests conducted over twenty-four hours and ten iterations within a simulated 6 × 6 km area. These evaluations rigorously tested the framework's response under a variety of network conditions and sophisticated attack scenarios, ranging from low to high density networks involving 01 to 1500 nodes, rapid changes in vehicle speeds, and environments mimicking urban intermittent connectivity and constant movement on highways.

In-depth simulations of attacks such as Sybil for testing resilience against false identity creation, GPS spoofing for assessing the system's capability to detect and correct location falsifications, and replay attacks to evaluate the effectiveness in handling repeated transmissions of old data were integral parts of the testing phase. The Scalable Wireless Ad-Hoc Network Simulator (SWANS) Ulm Highway model [25], which supports a highway scenario with three lanes where vehicles could achieve speeds of up to 50 m/s, with an average of 40 m/s, was implemented. This model accurately simulated complex driving behaviors, including collision avoidance and lane switching, providing a robust basis for assessing vehicular communication dynamics.

The physical layer was set to accommodate Rayleigh fading and a TwoRay path loss model with a transmission power of 10.9 dB. The MAC layer was programmed with the 802.11p standard, crucial for enabling Dedicated Short-Range Communications (DSRC) within the 5.9 GHz band. The network was configured to support a maximum packet size of 3072 bytes. Beacons were configured to transmit every 0.1 s, each with a size of 300 bytes, and utilized varied sketch sizes and the hash method (SHA-256), optimizing the handling of vehicle locations and payload data. These detailed configurations and extensive testing protocols provided crucial insights into the performance and communication dynamics (i.e., as exhibited in Figure 8) under different vehicular densities and mobility conditions in the network.



(**a**) Session creation (**b**) Connection initiation (**c**) Packet exchanges

(**d**) Alert generation (**e**) Global report export (**f**) D-CASPBR scan strength

(**g**) New node joining pattern (**h**) DDoS attack attempts (**i**) Session connection disconnections

Figure 8. Emulation processes in the controlled environment.

Our research also focused on understanding how the length of wireless communication links impacts message loss rates. As exhibited in Figure 9, we observed that longer links were prone to higher loss rates due to increased signal attenuation, multi-path fading, and interference, which were more evident as the link distances extended. The constant and rapid changes in vehicle positions led to significant variations in the lengths of communication links, which in turn affected the reliability and stability of data transmissions.

To tackle these challenges, our emulation employed the Low-Density Parity-Check (LDPC) coding scheme which was designed to enhance signal robustness over diverse distances. This technique leveraged a sparse parity-check matrix that effectively decoded incoming messages, drastically lowering the error rate. Correspondingly, our team integrated several network protocols: the Distance-Aware Rate Adjustment Strategy (DARAS), Density-Aware Transmission Power Control Protocol (DATPCP), and Dynamic Power Adjustment for Vehicular Networks (DPA-VN). These protocols were specifically developed to adapt transmission power and dynamically regulate the dissemination rate of messages, responding in real-time to the existing network density and the typical distance between vehicles. This adaptive methodology proved crucial in countering the negative impacts of variable link lengths on message loss. It facilitated the development of more robust communication strategies and guaranteed the dependable transfer of essential safety and operational information among vehicles.

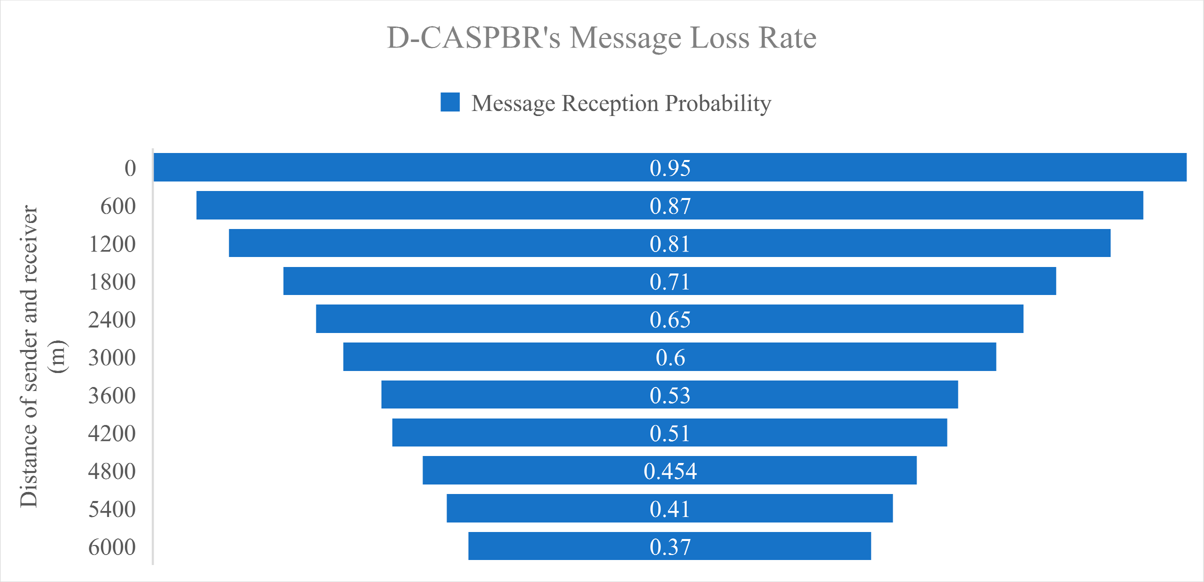


Figure 9. Influence of message loss rate on D-CASPBR.

Figure 9 displayed a distinct pattern: the message loss rate steadily escalated as the distance between sender and receiver increased from 0.6 km to 2.6 km, ranging from 2.4% to 4.4% and peaking at 4.95% at the shortest link when network density reached its maximum. This trend underscored the challenges presented by signal attenuation, multi-path fading, and interference, all of which intensified over longer distances and higher network densities. We observed that the application of the LDPC coding scheme, along with strategic network protocols such as DARAS and DPA-VN, successfully addressed these issues. Detailed analysis, as portrayed in Figure 8, confirmed that these technological adjustments not only enhanced signal robustness across varying distances but also maintained the stability and reliability of rapidly evolving vehicle-to-vehicle communications.

The efficacy of the D-CASPBR was heavily reliant on minimizing message loss rates to sustain the integrity and responsiveness of the network's threat detection system. Our studies showed that an increase in message loss corresponded with heightened latency in anomaly detection, which could compromise the network's security posture. To counter this, we enhanced our network protocols by incorporating advanced error-correcting codes and adaptable transmission power controls which proved to be an essential element for boosting network reliability. Key optimization parameters included the strength of error correction, the coding rate of advanced error-correcting codes, transmission range, signal strength, and various environmental factors influencing transmission power control. These upgrades significantly bolstered the dependability of transmitting crucial security alerts, thereby markedly reducing the likelihood of missed or delayed threat detections and strengthening the overall security framework of the network.

Figure 10 demonstrated that an increase in the number of nodes significantly enhanced spatial coverage, which facilitated more comprehensive monitoring and data collection within the proposed framework. Each node functioned as a sensor which enhanced the overall detection capabilities of the system. The expansion in node count not only improved redundancy in data collection and anomaly detection but also mitigated the risks associated with single points of failure to ensure the network maintained its integrity without significant blind spots.

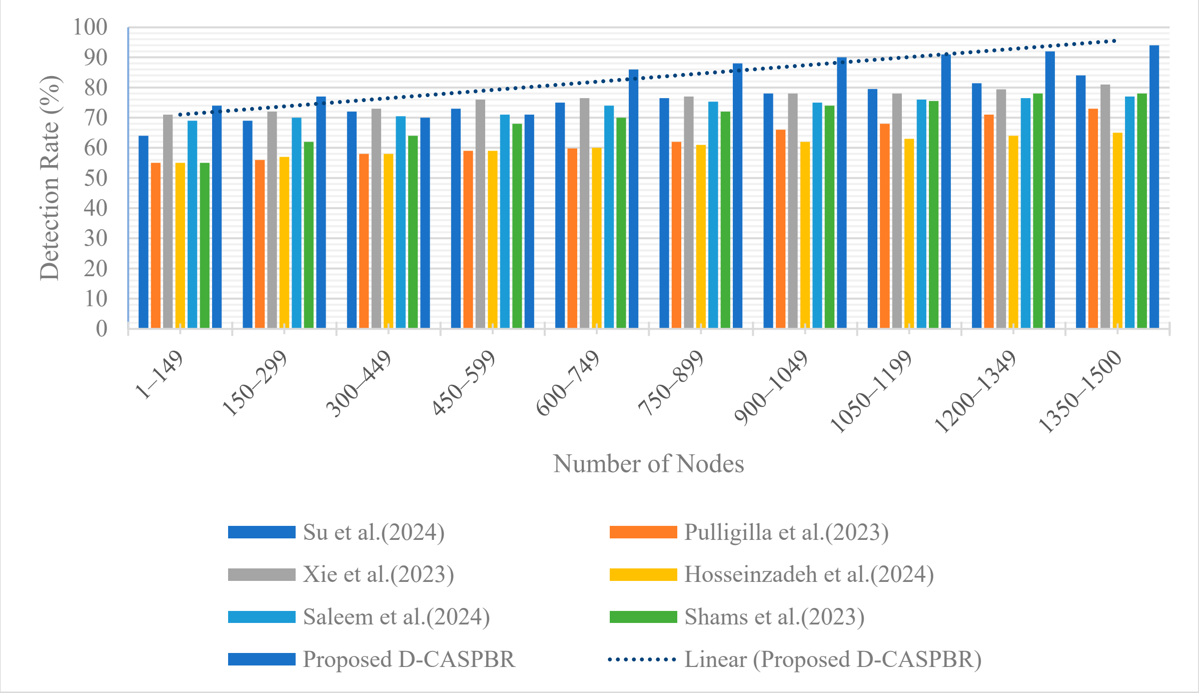


Figure 10. Investigating the impact of nodes on DDoS anomaly detection rates [6,7,9,12,17,20].

The addition of rapidly joining ingress and egress nodes brought diverse observational perspectives and heuristics which enriched the collective process of detecting anomalies. This diversity was instrumental in distinguishing normal network activities from genuine threats to effectively reduce false positives and enhancing the reliability of the anomaly detection system. Correspondingly, the increased node count bolstered the capacity for effective peer-to-peer communication and facilitated consensus building, which became a vital component in the decentralized system where the validation and response to detected anomalies relied on the concurrence of multiple nodes. Furthermore, the fact that the nodes were spread out across different locations meant that the network's structure was constantly changing and adapting. This made it much better at spotting unauthorized access attempts across a wider region. This capability was crucial for maintaining effective monitoring, even with the network's fast-paced, ever-changing nature. These strategic enhancements were integral in reinforcing the framework's ability to manage and mitigate potential security threats efficiently.

5. Conclusions

The proposed research has methodically engineered, deployed, and advanced robust DDoS mitigation strategies and a novel detection framework that was explicitly optimized for VANET environments. Through comprehensive analysis of the existing literature and emulation assessments, we demonstrated the efficacy of our methodologies in mitigating the impact of malicious attacks, highlighting the importance of robust security measures in safeguarding V2X communications, particularly in safety-critical applications. Leveraging advanced statistical analysis, fog computing, SD-VANETs, permissioned blockchain, and the hybrid machine learning technique, our approach offers a proactive defense mechanism against evolving threats that ensures the uninterrupted flow of vital information within vehicular networks. Our study contributes novel insights and methodologies addressing the unique challenges posed by DDoS attacks (e.g., but not limited to the following: GPS spoofing, gray-hole attacks, etc.), providing a tailored solution that enhances network resilience. Future research should aim to address limitations, such as further investigation into scalability and adaptability, exploring integration with existing security frameworks, and evaluating performance in real-world scenarios. While our proposed methodology has shown promising results, considerations such as a focus on specific DDoS attack types and scalability require further exploration to ensure effectiveness in large-scale VANET deployments.

Funding: The funding for this research is from the Deanship of Scientific Research at Prince Sattam bin Abdulaziz University under the research project '2024/01/28947'.

Institutional Review Board Statement: The study was conducted according to the guidelines of the Declaration of Deanship of Scientific Research, Prince Sattam bin Abdulaziz University.

Informed Consent Statement: This research did not involve human participants or animals; therefore, it was exempt from the requirements of ethics committee approval.

Data Availability Statement: The raw data supporting the conclusions of this article will be made available by the authors on request.

Conflicts of Interest: The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: U.T. reports financial support, administrative support, and article publishing charges were provided by Prince Sattam bin Abdulaziz University.

References

1. Li, J.; Xu, R.; Liu, X.; Ma, J.; Chi, Z.; Ma, J.; Yu, H. Learning for Vehicle-to-Vehicle Cooperative Perception Under Lossy Communication. *IEEE Trans. Intell. Veh.* **2023**, *8*, 2650–2660. [CrossRef]
2. Wang, J.; Zheng, Y.; Wang, J.; Shen, Z.; Tong, L.; Jing, Y.; Luo, Y.; Liao, Y. Ultra-Reliable Deep-Reinforcement-Learning-Based Intelligent Downlink Scheduling for 5G New Radio-Vehicle to Infrastructure Scenarios. *Sensors* **2023**, *23*, 8454. [CrossRef] [PubMed]
3. Chen, H.; Liu, J.; Wang, J.; Xun, Y. Towards secure intra-vehicle communications in 5G advanced and beyond: Vulnerabilities, attacks and countermeasures. *Veh. Commun.* **2023**, *39*, 100548. [CrossRef]
4. Karabulut, M.A.; Shah, A.F.M.S.; Ilhan, H.; Pathan, A.-S.K.; Atiquzzaman, M. Inspecting VANET with Various Critical Aspects—A Systematic Review. *Ad Hoc Netw.* **2023**, *150*, 103281. [CrossRef]
5. Nagarajan, J.; Mansourian, P.; Shahid, M.A.; Jaekel, A.; Saini, I.; Zhang, N.; Kneppers, M. Machine Learning based intrusion detection systems for connected autonomous vehicles: A survey. *Peer-to-Peer Netw. Appl.* **2023**, *16*, 2153–2185. [CrossRef]
6. Su, H.; Dong, S.; Wang, N.; Zhang, T. An efficient privacy-preserving authentication scheme that mitigates TA dependency in VANETs. *Veh. Commun.* **2024**, *45*, 100727. [CrossRef]
7. Pulligilla, M.K.; Vanmathi, C. An authentication approach in SDN-VANET architecture with Rider-Sea Lion optimized neural network for intrusion detection. *Internet Things* **2023**, *22*, 100723. [CrossRef]
8. Santhi, G.B.; Jacob, S.S.; Sheela, D.; Kumaran, P. Traffic coordination by reducing jamming attackers in VANET using probabilistic Manhattan Grid Topology for automobile applications. *Sci. Rep.* **2024**, *14*, 8365. [CrossRef]
9. Xie, Q.; Ding, Z.; Zheng, P. Provably Secure and Anonymous V2I and V2V Authentication Protocol for VANETs. *IEEE Trans. Intell. Transp. Syst.* **2023**, *24*, 7318–7327. [CrossRef]
10. Nobahari, A.; Avval, D.B.; Akhbari, A.; Nobahary, S. Investigation of Different Mechanisms to Detect Misbehaving Nodes in Vehicle Ad-Hoc Networks (VANETs). *Secur. Commun. Netw.* **2023**, *2023*, 4020275. [CrossRef]

11. Zemmoudj, S.; Bermad, N.; Bouallouche-Medjkoune, L. Detection and mitigation of vehicle platooning disruption attacks. *Veh. Commun.* **2024**, *47*, 100765. [CrossRef]
12. Hosseinzadeh, M.; Servati, M.R.; Rahmani, A.M.; Safkhani, M.; Lansky, J.; Janoscova, R.; Ahmed, O.H.; Tanveer, J.; Lee, S.-W. An Enhanced Authentication Protocol Suitable for Constrained RFID Systems. *IEEE Access* **2024**, *12*, 61610–61628. [CrossRef]
13. Sumit; Chhillar, R.S.; Dalal, S.; Dalal, S.; Lilhore, U.K.; Samiya, S. A dynamic and optimized routing approach for VANET communication in smart cities to secure intelligent transportation system via a chaotic multi-verse optimization algorithm. *Clust. Comput.* **2024**, *27*, 7023–7048. [CrossRef]
14. Kuriakose, J.; Joshi, S.; Bairwa, A.K. EMBN-MANET: A method to Eliminating Malicious Beacon Nodes in Ultra-Wideband (UWB) based Mobile Ad-Hoc Network. *Ad Hoc Netw.* **2023**, *140*, 103063. [CrossRef]
15. Shawky, M.A.; Shah, S.T.; Abdrabou, M.; Usman, M.; Abbasi, Q.H.; Flynn, D.; Imran, M.A.; Ansari, S.; Taha, A. How Secure Are Our Roads? An In-Depth Review of Authentication in Vehicular Communications. *Veh. Commun.* **2024**, *47*, 100784. [CrossRef]
16. Verma, A.; Saha, R.; Kumar, G.; Kim, T.-H. The Security Perspectives of Vehicular Networks: A Taxonomical Analysis of Attacks and Solutions. *Appl. Sci.* **2021**, *11*, 4682. [CrossRef]
17. Saleem, M.A.; Li, X.; Mahmood, K.; Shamshad, S.; Ayub, M.F.; Bashir, A.K.; Omar, M. Provably Secure Conditional-Privacy Access Control Protocol for Intelligent Customers-Centric Communication in VANET. *IEEE Trans. Consum. Electron.* **2024**, *70*, 1747–1756. [CrossRef]
18. Souissi, I.; Abidi, R.; Ben Azzouna, N.; Berradia, T.; Ben Said, L. ECOTRUST: A novel model for Energy COnsumption TRUST assurance in electric vehicular networks. *Ad Hoc Netw.* **2023**, *149*, 103246. [CrossRef]
19. Khalid, W.; Ahmed, N.; Khan, S.; Ullah, Z.; Javed, Y. Simulative Survey of Flooding Attacks in Intermittently Connected Vehicular Delay Tolerant Networks. *IEEE Access* **2023**, *11*, 75628–75656. [CrossRef]
20. Shams, E.A.; Rizaner, A.; Ulusoy, A.H. Flow-based intrusion detection system in Vehicular Ad hoc Network using context-aware feature extraction. *Veh. Commun.* **2023**, *41*, 100585. [CrossRef]
21. Masood, S.; Saeed, Y.; Ali, A.; Jamil, H.; Samee, N.A.; Alamro, H.; Muthanna, M.S.A.; Khakimov, A. Detecting and Preventing False Nodes and Messages in Vehicular Ad-Hoc Networking (VANET). *IEEE Access* **2023**, *11*, 93920–93934. [CrossRef]
22. Jin, R.; Zhang, G.; Hsu, L.-T.; Hu, Y. A Survey on Cooperative Positioning Using GNSS Measurements. *IEEE Trans. Intell. Veh.* **2024**, 1–20. [CrossRef]
23. Karthik, M.G.; Krishnan, M.B.M. Hybrid random forest and synthetic minority over sampling technique for detecting internet of things attacks. *J. Ambient. Intell. Humaniz. Comput.* **2021**, 1–11. [CrossRef]
24. James, D. OMNeT++ Discrete Event Simulator. *Simulator*. 28 February 2024. Available online: https://omnetpp.org/ (accessed on 4 June 2024).
25. Parsa, A.; Moghim, N.; Haghani, S. Joint congestion and contention avoidance in a scalable QoS-aware opportunistic routing in wireless ad-hoc networks. *PLoS ONE* **2023**, *18*, e0288955. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.