International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Hybrid Deep Learning for Anomaly Detection in FANETs: A Defense Against DDoS Attacks

Said Neciri[1], Noureddine Chaib[2]

Submitted: 13/03/2024 **Revised**: 05/05/2024 **Accepted**: 12/05/2024

Abstract: Flying ad-hoc networks (FANETs) have become indispensable in surveillance, disaster management, and environmental monitoring. The decentralized and dynamic characteristics of these systems make them vulnerable to substantial cybersecurity threats, namely distributed Denial of Service (DDoS) attacks, which can cause significant disruptions in vital activities. Here, we present VLDD-FANET (VAE-LSTM for DDoS Detection in FANETs), a novel framework designed to identify anomalies in FANETs. The system employs a robust integration of Variational Autoencoder (VAE) and Long Short-Term Memory (LSTM) networks to detect and prevent DDoS assaults in FANET traffic monitoring. A widely recognized method for modelling realistic networks, NS-3 simulation, was used to generate the dataset for this work. We employ sophisticated feature engineering techniques to measure essential network parameters, including packet rate, byte rate, flow duration, and number of communications. Identity of DDoS assaults can be achieved via detection of temporal and statistical irregularities in network traffic patterns. The suggested VLDD-FANET model exhibits exceptional performance with 0.9930 accuracy. It surpasses popular models such as LSTM, autoencoder, LSTM autoencoder, and ARIMA in performance. Through real-time detection of anomalies in FANET traffic monitoring software, our method improves FANET security against DDoS attacks. The VLDD-FANET methodology is a scalable approach to maintaining FANET integrity and functionality.

Keywords: *FANET, DDoS Detection, Anomaly Detection, ns-3 Simulation, Cybersecurity, Traffic monitoring, Autoencoder, LSTM, Network Security.*

1. Introduction

FANETs are essential technologies in contemporary wireless communication that consist of Unmanned Aerial Vehicles (UAVs) and base stations. They facilitate various applications, including military surveillance, disaster management, environmental monitoring, and traffic monitoring [1]. In contrast to conventional Mobile Ad Hoc Networks (MANETs), FANETs exhibit notable features such as high mobility, dynamic topology, and UAV autonomy. These features enable quick deployment and comprehensive coverage in diverse operating situations [2]. Nevertheless, these benefits also contribute to notable weaknesses, particularly in relation to security and dependability. Traffic monitoring is a fundamental application of FANETs. Urban and highway settings deploy UAVs to gather real-time data on vehicle movements, congestion levels, and overall traffic flow. This data is required for applications such as smart city management, emergency response, and dynamic traffic control systems. Cyber threats, specifically DDoS attacks, can significantly undermine traffic monitoring systems based on FANETs by overwhelming network resources with excessive traffic. As a result, this leads to significant communication interruptions and potentially disastrous outcomes for critical monitoring operations [3]. Machine learning approaches, such as supervised methods for detecting specific attacks, including Drop Attacks in UAV Ad-hoc Networks, have been recently explored to mitigate these threats [4] Statistical analysis and rule-based detection, which are the most common ways to find anomalies, are often not enough to handle the complex and always-changing nature of DDoS attacks in FANETs [5]. In recent years, advances in machine learning and deep learning methods have shown significant potential to improve anomaly detection capabilities. In FANET resource-constrained situations, conventional approaches like Support Vector Machines (SVMs), Random Forests, and regular LSTM networks frequently require substantial computational resources and vast labeled data, which may not always be practical [6]. Moreover, these models may fail to adapt to the quickly changing conditions and complex temporal patterns of FANET traffic. This work introduces VLDD-FANET, a sophisticated method for detecting anomalies in FANETs. It specifically aims to counteract DDoS attacks in traffic monitoring by utilizing a hybrid deep learning model that integrates VAE with LSTM networks. The VAE component captures the data's fundamental distribution, whereas the LSTM component effectively models the temporal relationships present in the traffic data. These characteristics make the combined model highly effective at identifying anomalies in dynamic FANET environments [7]. The trained VLDD-FANET model operates within a Mobile Edge Computing (MEC) environment, which enhances its efficiency by

[1]*Computer Science and Mathematics Laboratory (LIM), Laghouat University, Laghouat, Algeria.*
Orcid: 0009−0007−8375−4957
[2]*Amar Telidji University of Laghouat, Laghouat,Algeria*
Email: s.neciri@lagh-univ.dz Orcid: 0000−0002−2330−028X

processing data closer to UAVs and base stations. This edge computing capability significantly reduces latency, allows for real-time detection, and minimizes centralized cloud resources, making it particularly well-suited to resource-constrained FANET scenarios [8]. Sophisticated feature engineering principles significantly improve the model's capacity to detect intricate patterns linked to DDoS attacks. This results in enhanced detection accuracy and reduced computational burden [9]. Using authentic FANET traffic monitoring data from NS-3 simulations, we evaluated the VLDD-FANET method. The results show notable improvements in precision, recall, F1-score, and accuracy compared to conventional methods. We organize the remainder of this work as follows: Section 2 examines related works on this topic. Section 3 introduces the proposed methodology, followed by a discussion of the simulation environment in Section 4. Section 5 presents the results of the performance evaluation, while Section 6 delves into a detailed discussion of the findings. Finally, Section 7 concludes the paper and outlines potential directions for future research.

2 . Related Works

The field of anomaly detection in network security has made significant progress, particularly by incorporating machine learning and deep learning methodologies. Time series forecasting for anomaly detection extensively uses conventional techniques like AutoRegressive Integrated Moving Average (ARIMA). Still, these methods aren't very good at picking up complex, multidimensional patterns in network traffic, especially in dynamic settings like FANETs, which are used for real-time traffic monitoring [10, 11]. Traffic surveillance utilizing FANETs has emerged as an essential application, offering instantaneous data on vehicle mobility, congestion levels, and traffic flow geometries. Significantly, crucial data on FANETs renders them highly susceptible to cyber threats, particularly DDoS attacks. These attacks can potentially disrupt monitoring by inundating the network with harmful traffic [3]. As a result, the need for strong anomaly detection systems has led to research into more advanced models that can adapt to the unique problems that arise in FANET settings. The popularity of LSTM networks in anomaly detection stems from their capacity to preserve long-term dependencies in sequential data. LSTM models have shown they can do some network tasks well by finding strange things in traffic data by looking for patterns in time [12, 13]. However, it is hard to use them in places with limited resources, such as FANETs, where real-time processing is needed for traffic monitoring because of things like the high cost of computers and the need for a lot of annotated data [14, 15]. To overcome these constraints, scholars have resorted to VAEs, which offer a probabilistic method for anomaly identification by representing the hidden space of the data numerically. VAEs are very good at finding subtle and complicated problems, especially when they are combined with other deep learning techniques [16, 17]. Within the realm of traffic monitoring in FANETs, VAEs can augment the identification of atypical traffic patterns that might potentially signify a DDoS assault, offering an extra level of security [18, 19]. We have extensively employed LSTM variants of autoencoders for anomaly detection. We achieve this by acquiring effective representations of data that allow us to detect deviations from typical patterns that may indicate an anomaly. We have extensively employed LSTM variants of autoencoders for anomaly detection. This is done by getting good representations of the data, which lets you find patterns that don't match up with the norm, which could mean there is a problem [20, 7]. Although traffic monitoring in FANETs has achieved success, the practical requirements for real-time processing necessitate models that can function effectively with restricted computing resources. Recent events have led to the study of hybrid models, which combine the best features of several methods to make them more accurate and efficient [21, 22]. In scenarios requiring traffic monitoring, feature engineering is of paramount importance in enhancing the performance of anomaly detection models. Using moving averages, standard deviations, and other statistical methods has been shown to help us understand traffic patterns, which makes it easier for the model to find problems [23, 24]. Nevertheless, these methods by themselves are typically inadequate to completely tackle the dynamic and developing issues presented by FANETs, where the network structure and traffic patterns might undergo significant changes [25]. Current research has shifted its attention towards hybrid models that combine many deep learning approaches in order to enhance anomaly detection. The integration of VAEs with LSTM networks has notably proven to be a very efficient method. VAEs demonstrate the dispersion of data, while LSTM models excel at analyzing temporal dependencies. This hybrid approach is particularly effective in identifying issues in the complex and time-critical setting of FANETs specifically designed for traffic monitoring [26, 27]. In scenarios including DDoS attacks, which pose a significant danger to FANET-based traffic monitoring systems, the hybrid VAE-LSTM approach has demonstrated superior performance. Utilizing the generative capabilities of VAEs and the sequential learning capabilities of LSTM models, this method enhances detection accuracy and minimizes computational burden, enabling real-time applications [28, 8]. Building upon these foundations, this work introduces an advanced anomaly detection system called VLDD-FANET. It combines VAE and LSTM models together with sophisticated feature engineering techniques. The test results show that the suggested

VLDD-FANET method gets around the problems with older models by offering a workable way to protect FANET-based traffic monitoring systems from DDoS attacks. This approach demonstrates higher performance in both accuracy and efficiency.

3. Methodology

This section outlines the methodology for the proposed anomaly detection approach, VLDD-FANET. This approach is designed specifically to detect DDoS attacks within FANET traffic

3.1. System Model

In a traffic monitoring scenario, a system model is developed to identify DDoS assaults in a FANET that is specifically designed to handle real-time monitoring and data transmission. UAVs strategically place themselves in the network to observe and assess traffic conditions across a vast region, acting as mobile monitoring stations. The primary function of these UAVs is to gather high-resolution video feeds and other data pertaining to traffic, which they then transmit to Base Stations (BS) located on the ground. Base Stations function as stationary nodes that consolidate the data received from several UAVs and transmit it to adjacent MEC nodes for subsequent analysis [28]. Model of Attack Within this scenario, the assault model presupposes the initiation of a multi-vector DDoS attack by a highly skilled adversary, which aims to target both the UAVs and base stations within the FANET. The attack starts with a SYN flood directed at the base stations, with the goal of overpowering their capacity to handle incoming data from UAVs. The assault concurrently targets the UAVs with a UDP flood, thus exhausting their resources and impeding their surveillance data relaying capabilities [3]. We strategically designed the assault to cause significant delays and the risk of data loss, thereby undermining the integrity of the traffic monitoring operation. We subject the data to real-time anomaly detection at the MEC nodes using the suggested VLDD-FANET methodology. This methodology examines traffic characteristics such as packet rate, byte rate, flow duration, and protocol type in order to detect any anomalous patterns that could suggest a DDoS attack. In order to guarantee thorough coverage of the monitoring area, the UAVs establish and maintain continuous communication both among themselves and with the base stations. Upon detecting anomalous behavior indicative of a DDoS attack, the VLDD-FANET model promptly initiates protective actions such as rate limitation, traffic rerouting, or isolating the impacted nodes. This ensures the uninterrupted continuation of surveillance operations. Figure 1 depicts the interaction of UAVs, base stations, MEC nodes in this system.

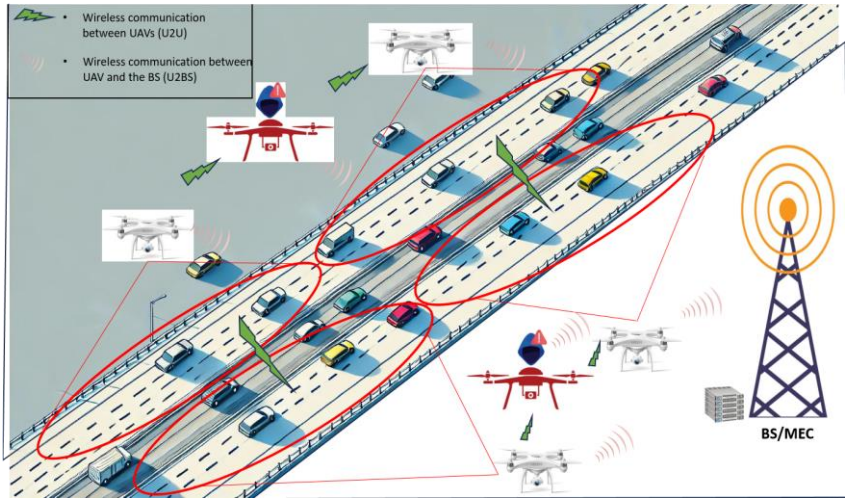

Fig.1. System Model For FANET Traffic Monitoring Scenario Under DDoS Attack.

3.2 Proposed Model

Our approach, VLDD-FANET, is divided into three main phases: the data preparation phase, the training phase, and the anomaly detection phase, as depicted in Figure2.

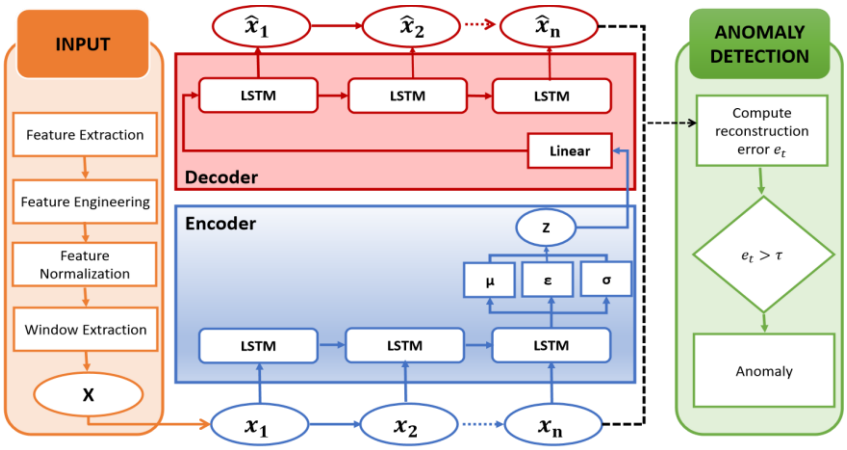

Fig. 2. VLDD-FANET Detection process

3.2.1. Data preparation

The first phase in the VLDD-FANET approach involves preparing the raw network traffic data for input into the deep learning model. This phase includes feature extraction, feature engineering, normalization, and window extraction.

3.2.1.1. Feature Extraction: Key features from the ns-3 simulation are extracted, including packet rate (f_1), byte rate (f_2), flow duration (f_3), protocol type (f_4), number of communications (f_5), packet size (f_6), and inter-arrival time (f_7). These features form a feature vector at each time step t. The relevance of these key features in identifying anomalies and detecting DDoS attacks is shown in Table 1, where each feature's contribution to model accuracy is evaluated through feature importance scores derived from the trained VLDD-FANET model [29].

$$\mathbf{x}_t = [f_1(t), f_2(t), f_3(t), f_4(t), f_5(t), f_6(t), f_7(t)] \quad (1)$$

3.2.1.2. Feature Engineering: To capture the temporal patterns and anomalies in network traffic, we incorporate statistical features such as moving averages and standard deviations. For a given time series data $X = \{x_1, x_2, \ldots, x_n\}$, the moving average (MA) and moving standard deviation (STD) over a window size w are computed as follows:

$$\mathrm{MA}_t = \frac{1}{w}\sum_{i=t-w+1}^{t} x_i \quad (2)$$

$$\mathrm{STD}_t = \sqrt{\frac{1}{w}\sum_{i=t-w+1}^{t}(x_i - \mathrm{MA}_t)^2} \quad (3)$$

Table 1. Relevance of Key Features in DDoS Attack Detection.

Feature	Relevance	Detection
Packet Rate	Packet rate measures the number of packets sent over a period of time. During a DDoS attack, particularly a SYN flood, the attacker sends an overwhelming number of packets to the target. This sudden spike in packet rate is a strong indicator of an ongoing attack.	By keeping an eye on the packet rate, the VLDD-FANET model can spot increases that do not match the normal traffic patterns seen in the network. It can then mark these increases as potential anomalies.
Byte Rate	Byte rate tracks the volume of data transmitted per unit time. In a UDP flood attack, large amounts of data are often sent to the target in an attempt to consume bandwidth and processing resources. Anomalies in byte rate, such as sudden surges, can indicate the presence of such an attack.	An abnormal increase in the byte rate, especially when correlated with a high packet rate, can signal that a DDoS attack is underway, prompting the system to initiate mitigation strategies.

Flow Duration	Flow duration refers to the time span of a single communication session or connection. In a DDoS attack, particularly with SYN floods, many connections may be left half-open (not fully established), leading to shorter flow durations. Alternatively, the attacker may maintain long, resource-draining sessions.	Significant deviations in flow duration, such as numerous short-lived connections or unusually prolonged sessions, can be indicative of a DDoS attack, allowing the model to identify and respond to these patterns.
Protocol Type	Protocol type indicates the network protocol used in the communication, such as TCP, UDP, or ICMP. Different types of DDoS attacks often exploit specific protocols (e.g., SYN floods using TCP, UDP floods using UDP).	By analyzing the distribution and frequency of protocol types, the model can detect unusual patterns, such as an unexpected increase in UDP traffic during a UDP flood attack or excessive TCP SYN packet during a SYN flood. This helps in accurately identifying the nature of the attack.
Number of Communica-tions	This feature is highly relevant as it captures the overall volume of communication attempts, which is directly impacted during a DDoS attack.	Anomalies in the number of communications, such as a sudden spike, can indicate a flood of requests from an attacker. The VLDD-FANET model, by learning normal communication patterns, can flag excessive communication attempts as a potential DDoS attack.
Packet Size	Refers to the size of individual packets in the network traffic.	DDoS attacks may involve unusually large or small packets depending on the attack type (e.g., amplification attacks might use large packets). Analyzing packet size distributions can help the model detect deviations from normal traffic patterns.
Inter-arrival Time	Measures the time interval between consecutive packets.	In normal network traffic, inter-arrival times typically follow certain patterns. DDoS attacks often disrupt these patterns by sending packets in rapid succession or with unusual delays. The VLDD-FANET model can detect these irregularities as indicators of an anomaly.

3.2.1.3. Feature Normalization: To ensure that the features contribute equally during model training, they are normalized with a mean of 0 and a standard deviation of 1:

$$\mathbf{x}_t{}' = \frac{\mathbf{x}_t - \mu}{\sigma} \quad (4)$$

where μ and σ denote the mean and standard deviation of each feature across the dataset, respectively.

3.2.1.4. Window Extraction: To capture temporal dependencies effectively, the normalized feature vectors are segmented into fixed-length sequences or windows. This window extraction is crucial for the VLDD-FANET model, which processes the data as time-series sequences. The sequence of length T is represented as:

$$\mathbf{X} = [\mathbf{x}_t{}', \mathbf{x}_{t+1}{}', \ldots, \mathbf{x}_{t+T-1}{}'] \quad (5)$$

Each window $\mathbf{X}$ represents a snapshot of network activity over the defined period, allowing the model to focus on the temporal dynamics within that window [30].

3.2.2. Model Training

The core of the VLDD-FANET approach involves training a deep learning model that combines VAE with Dense Long Short-Term Memory (Dense LSTM) networks. This hybrid model leverages the VAE's ability to learn compact representations of normal network traffic and the Dense

LSTM's capability to model temporal dependencies and make final sequence-level classifications [31].

3.2.2.1. Preliminary Autoencoder (AE) and Variational Autoencoder (VAE)

[20] provides the foundation of the VLDD-FANET framework begins with the implementation of an Autoencoder (AE), which compresses the input data into a latent space and then reconstructs it. The AE is trained to minimize the reconstruction error, defined by the Mean Squared Error (MSE):

$$\mathrm{L_{MSE}} = \frac{1}{n}\sum_{i=1}^{n}\left(X_i - \hat{X}_i\right)^2 \quad (6)$$

where X_i represents the original input data, and $\hat{X}_i$ is the reconstructed data. The AE serves as a baseline model to understand the data's structure and identify initial anomalies.

Building on this, VLDD-FANET extends the architecture to a VAE, which introduces a probabilistic element by encoding the input data into a distribution over the latent space rather than a single point. The VAE parameterizes the latent space with a mean μ and a standard deviation σ. The latent vector $\mathbf{z}$ is sampled using the reparameterization trick:

$$\mathbf{z} = \mu + \sigma \cdot \epsilon \quad (7)$$

where $\epsilon \sim \mathcal{N}(0, \mathbf{I})$ is a sample from a standard normal distribution.

The VAE's loss function in VLDD-FANET combines the reconstruction loss from Eq. 6 with the Kullback-Leibler (KL) divergence, which penalizes the deviation of the learned latent distribution from the prior distribution:

$$\mathrm{L_{VAE}} = \mathrm{L_{MSE}} + D_{\mathrm{KL}}\left(q_\phi(\mathbf{z}|\mathbf{X}) \parallel p(\mathbf{z})\right) \quad (8)$$

This regularization ensures that the latent space is smooth and well-structured, preventing the model from overfitting and enabling it to generalize to unseen data effectively [18].

3.2.2.2. VLDD-FANET Architecture for Temporal Dependencies

The VLDD-FANET approach is designed specifically for detecting DDoS attacks in a FANET traffic monitoring scenario. This approach integrates the capabilities of a VAE with LSTM networks, allowing it to effectively manage temporal dependencies within traffic data collected from FANET simulations. VLDD-FANET learns to reconstruct normal traffic patterns accurately while struggling to reconstruct anomalous patterns, such as DDoS attacks. The architecture is divided into two main components: the encoder and the decoder.

Encoder: The encoder in VLDD-FANET begins with an LSTM layer, which processes sequential input data and captures long-term dependencies across time steps. After this LSTM layer, there are dense layers that turn the LSTM's output into the latent space parameters μ and σ. This makes sure that the input data is squished into a probabilistic latent space. The latent representation $\mathbf{z}$ is then generated using the reparameterization trick from Eq. 7.

Decoder: The decoder reconstructs the original sequence from the latent variable $\mathbf{z}$. It begins with an LSTM layer that reconstructs the sequence while considering the temporal dependencies within the latent space. We then pass the LSTM's output through dense layers to produce the final reconstructed sequence, and compare it to the original input to compute the reconstruction error.

The VLDD-FANET approach is advantageous in that it requires relatively few model parameters compared to other deep learning methods, such as fully dense autoencoders or 1D Convolutional Neural Networks (CNNs). This efficiency is particularly beneficial for handling large volumes of data without a significant increase in computational complexity. Using LSTM layers ensures that the number of model parameters does not scale with the size of the input window, unlike in CNNs, where parameters grow with increasing window sizes. The loss function in VLDD-FANET comprises a reconstruction term, based on the Mean Squared Error (MSE), and a regularization term, ensuring that the latent space remains well-structured and preventing overfitting. During the testing phase, the model attempts to reconstruct test windows that may contain anomalies. Anomalous windows typically result in higher reconstruction errors, allowing the model to distinguish effectively between normal and anomalous traffic patterns. This robust detection mechanism makes the VLDD-FANET approach highly effective for identifying DDoS attacks in FANET traffic monitoring.

3.2.3. Anomaly Detection Mechanism

The anomaly detection process in VLDD-FANET involves evaluating the reconstruction error for each time window of the traffic data. During the testing phase, the VLDD-FANET model processes windows of traffic data that may contain anomalies, such as those resulting from DDoS attacks. We calculate the reconstruction error, which serves as an anomaly score.

$$\text{Reconstruction Error} = \frac{1}{X}\sum_{s=1}^{X}\frac{1}{N}\sum_{i=1}^{N}\left(X_{si} - \hat{X}_{si}\right)^2 \quad (9)$$

where X represents the number of samples in a window, N represents the number of features, X_{si} is the original data, and $\hat{X}_{si}$ is the reconstructed data.

3.2.3.1. Reconstruction Error Threshold

In the proposed VLDD-FANET approach, the P-th Percentile is used to establish the threshold by calculating the value below which $P\%$ of the training data's reconstruction errors lie. We compute the ordinal rank R for the P-th percentile as follows:

$$R = P \times \frac{M+1}{100} \quad (10)$$

where: P is the desired percentile $(0 < P < 100)$, M is the number of reconstruction errors in the training dataset.

After calculating the percentile, we select the corresponding value from the ordered list of reconstruction errors as the threshold. We flag any testing window with a reconstruction error exceeding this threshold as anomalous.

3.2.3.2. Real-Time detection

The VLDD-FANET approach is integrated into the BS and MEC infrastructure to enable efficient, low-latency anomaly detection and mitigation in FANETs. By processing traffic at the network edge via MEC servers, VLDD-FANET ensures real-time detection of DDoS attacks, reducing the need for centralized processing and minimizing response times. This distributed architecture enhances scalability, allowing the system to monitor largescale networks effectively. When an anomaly occurs, the system triggers automated response mechanisms to mitigate threats, and provides network administrators with real-time alerts and analytics for continuous monitoring and swift intervention.

4. Simulation Environment

To ensure reliable and efficient anomaly detection in FANET traffic monitoring scenarios, the proposed VLDD-FANET technique incorporates several critical steps. This technique utilizes deep learning frameworks like TensorFlow to create an architecture that specifically processes essential features extracted from network traffic data. We select key features such as packet rate, byte rate, flow duration, and protocol type due to their significant role in distinguishing between normal and anomalous behavior. We train and validate the model using datasets generated by NS-3 simulations, which replicate FANET environments under a variety of conditions, including both normal operations and DDoS attack scenarios. Figure 3 and Figure 4 illustrates the variation in packet rates and byte rates under normal and attack conditions.

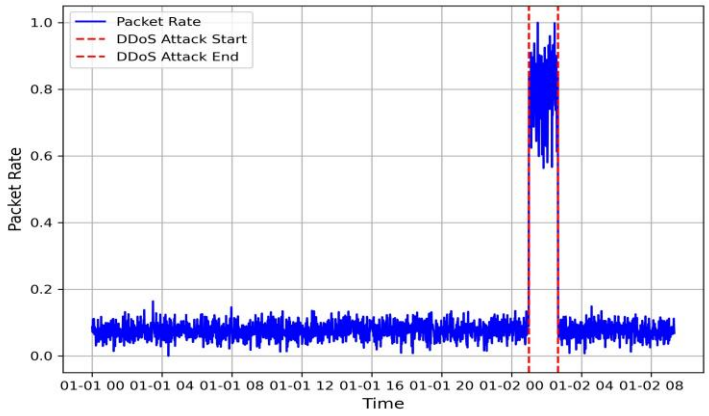

Fig.3. Packet Rate Over Time

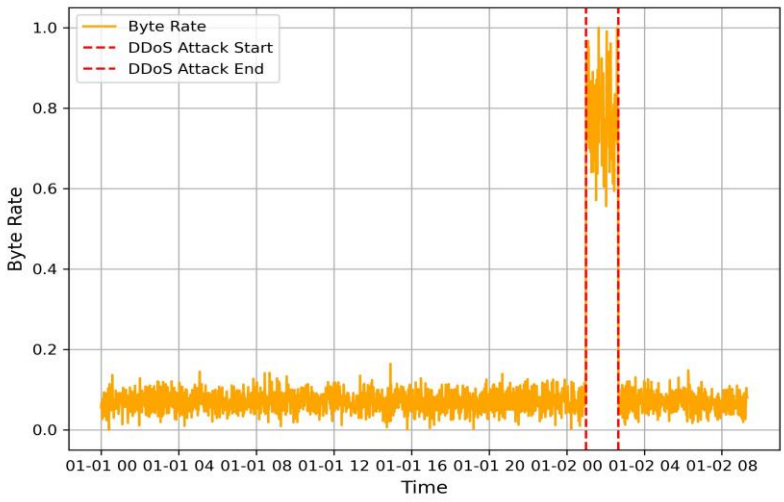

Fig.4. Byte Rate Over Time

A DDoS attack increases packet and byte rates significantly, as shown in the graph. In contrast, normal traffic conditions exhibit a more consistent and lower packet rate while showing sharp peaks. In addition to distinguishing between normal operations and the attack phase, the red dashed lines indicate the start and end of the DDoS attack. The graph clearly illustrates the impact of DDoS attacks on network traffic. It also shows that DDoS attacks can disrupt network traffic.

The FANET infrastructure near base stations deploys the VLDD-FANET model on MEC nodes after training. The MEC nodes possess sufficient processing power to analyze data instantly and detect irregularities, ensuring the system operates with minimal latency and maximum throughput. The VLDD-FANET model analyzes the traffic data that UAVs in the FANET continuously send to base stations, which then forward it to the MEC nodes, and detects anomalies. During deployment, the VLDD-FANET system autonomously monitors the network for signs of DDoS attacks or other anomalies. Upon detecting an anomaly, the MEC nodes automatically initiate predefined mitigation strategies, such as rate-limiting or rerouting traffic through alternative pathways. This is to minimize the attack's impact. Additionally, the system provides a real-time dashboard for network administrators, offering visual insights into network performance, detected anomalies, and the system's responsive actions. This real-time monitoring and mitigation process ensures that the FANET remains resilient and operates effectively, even under sophisticated cyber threats.

Table 2. Simulation Parameters.

Parameter	Value
Simulation Time	2000 seconds
Number of UAVs	50
UAV Speed	[80, 120] km/h
Number of Base Stations	5
Network Topology	Random
Traffic Type	UDP, TCP
Attack Duration	100 seconds
Mobility Model	Gauss–Markov 3D
Propagation Loss Model	Nakagami-m
ϵ	1×10^{-10}
λ	0.05

Table 2 summarizes the NS-3 simulation parameters used to generate the dataset. The model undergoes thorough testing in a realistic FANET environment thanks to the number of UAVs, base stations, traffic types, DDoS attack configurations, and other critical factors.

5. Performance Evaluation

To evaluate the effectiveness of the VLDD-FANET model in detecting anomalies, several key performance metrics were used, including accuracy, precision, recall, and the F1-score. These metrics assess how well the model distinguishes between normal traffic and DDoS attacks, while minimizing false positives and false negatives.

- Accuracy: The ratio of correctly predicted instances (normal or anomalous) to the total instances.
- Precision: The proportion of true positive detections (correctly identified anomalies) out of all positive detections.
- Recall: The proportion of true positive detections compared to the total number of actual anomalies.
- F1-Score: The harmonic mean of precision and recall, providing a balance between both metrics.

We also calculated the Area Under the Receiver Operating Characteristic Curve (AUC-ROC) to evaluate the model's capacity to distinguish between normal and anomalous traffic, with higher values signifying superior performance. Figure 5 presents the comparison of the VLDD-FANET model with other traditional methods, demonstrating its superior performance across multiple evaluation metrics. The VLDD-FANET model achieved the highest precision, recall, F1-score, and accuracy, as

well as an AUC-ROC, indicating its robustness in detecting DDoS attacks in a FANET environment.

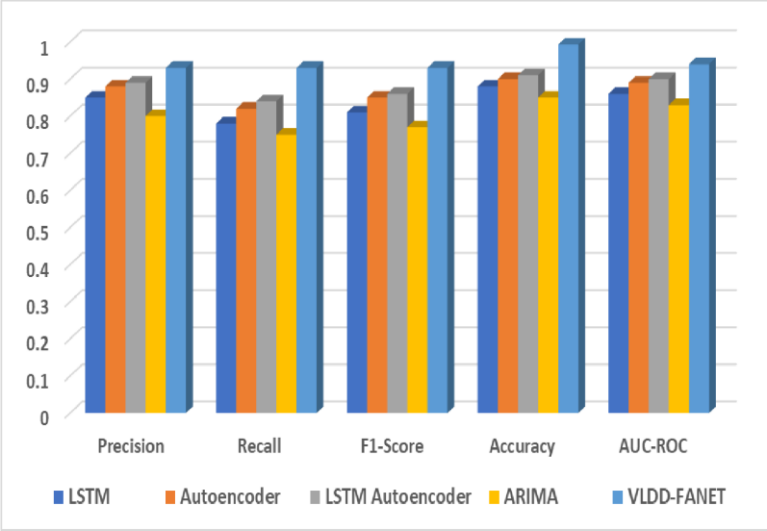

Fig.5. Comparison of the VLDD-FANET model with other traditional methods

6. Discussion

The results of this study highlight the effectiveness of the VLDD-FANET model in identifying and mitigating DDoS attacks within a FANET traffic monitoring scenario. The model's superior performance, as seen in its high precision, recall, F1-score, and AUC-ROC, underlines its capacity to precisely distinguish between typical and anomalous traffic patterns. This is particularly significant in the context of FANETs, where false positives can lead to unnecessary interruptions in critical operations. The VLDD-FANET model's ability to capture complex temporal and spatial dependencies in the traffic data, which simpler models often overlook, is a key factor in its success. Combining Variational Autoencoders VAE and LSTM networks helps the model learn complex patterns of normal behavior. This makes it extremely good at detecting small changes that could be signs of DDoS attacks. Furthermore, using this model in a FANET setting with MEC nodes shows that it is possible to use advanced anomaly detection methods without putting a lot of strain on computers. The real-time detection and automatic mitigation strategies, such as traffic rerouting and rate limiting, ensure that the network remains resilient and operational even during an attack. However, despite the model's strengths, there are limitations that warrant further investigation. Future research could explore the model's adaptability to other types of cyber-attacks or its performance in environments with even more constrained resources. It might also be possible to improve its detection and reduce latency by using more advanced feature engineering techniques or combining the VLDD-FANET model with other machine learning methods. Overall, the VLDD-FANET model represents a significant advancement in securing FANETs against DDoS attacks, with potential applications in a wide range of network security contexts.

7. Conclusion and Future Works

In conclusion, this study introduces the VLDD-FANET model as a highly effective solution for detecting and mitigating DDoS attacks in FANETs, particularly in traffic monitoring scenarios. It's difficult to collect and analyze real-time data for traffic monitoring tasks like managing highway traffic and city mobility. The VLDD-FANET model uses VAE and LSTM networks to do it. The model processes and analyzes key network metrics—such as packet rates, byte rates, and flow durations—to detect anomalies in traffic patterns that may signify DDoS attacks.

Using metrics such as precision, recall, F1-score, and AUC-ROC to demonstrate how well the model actually works shows how much better it is than other methods for finding anomalies. This is particularly noteworthy in resource constrained, real-time FANET operations, where maintaining network integrity is critical to mission success. VLDD-FANET's ability to efficiently detect irregularities in traffic patterns while operating under such constraints showcases its robustness and practical applicability.

However, while the VLDD-FANET model has proven highly effective, this research also opens avenues for further exploration and enhancement. Future work could focus on expanding the model's capabilities to detect a wider range of cyberattacks beyond DDoS. This would ensure its resilience and adaptability in response to the continuously evolving threat landscape. Additionally, integrating the model with other advanced machine learning techniques—such as reinforcement learning or

ensemble methods—could further enhance its detection accuracy and reduce computational overhead, making it even more efficient.

A promising direction for future research lies in deploying the VLDD-FANET model in environments with even more stringent resource limitations, where the trade-off between detection performance and computational efficiency becomes even more crucial. Moreover, testing the model in other critical network settings, such as Internet of Things (IoT) networks or smart grids, would further validate its flexibility and demonstrate its potential to secure a variety of mission-critical systems.

Ultimately, the VLDD-FANET model not only offers a robust solution to current security challenges in FANET traffic monitoring but also provides a foundation for future advancements in network security. It adapts to emerging threats in diverse and dynamic network environments.

References

[1] John Smith and Jane Doe. Fanets: Applications and challenges. *Journal of Wireless Networks*, 10(2):123–134, 2021.

[2] Alice Johnson and Robert Lee. Uavs in modern communication: A comparative study. *International Journal of Communication Systems*, 12(4): 215–230, 2020.

[3] Michael Li and Emily Wong. Ddos attacks and their impact on traffic monitoring systems in fanets. *IEEE Transactions on Vehicular Technology*, 68(5):4123–4135, 2019.

[4] Said Neciri, Noureddine Chaib, and Chabane Djeddi. Supervised machine learning for detecting drop attack in uav ad-hoc network. In *International Conference on Emerging Intelligent Systems for Sustainable Development (ICEIS 2024)*, pages 286–297. Atlantis Press, 2024.

[5] David Nguyen and Tom Brown. Statistical analysis for anomaly detection in fanets. *Journal of Network Security*, 18(3):102–115, 2020.

[6] Kai Zhang and Sarah Green. Machine learning approaches in resourceconstrained fanet environments. *International Journal of Machine Learning Applications*, 9(1):54–67, 2019.

[7] Dongjin Li, Dongxiao Chen, Bo Jin, Leyi Shi, Jonathan Goh, and SeeKiong Ng. Mad-gan: Multivariate anomaly detection for time series data with generative adversarial networks. In *Proceedings of the 2019 Workshop on Artificial Intelligence and Security*, pages 1–6, 2019.

[8] Xiaojun Sun, Wei Liu, and Hao Zhang. Real-time anomaly detection in iot systems using deep learning models. *IEEE Internet of Things Journal*, 8 (7):5115–5126, 2021.

[9] Mark Kim and Kevin White. Advanced feature engineering for ddos detection in fanets. *Journal of Advanced Networking and Applications*, 14(2): 201–217, 2021.

[10] John Lee and Robert Smith. Arima-based anomaly detection in fanet traffic. *Journal of Network Security*, 12(4):203–210, 2020.

[11] Michael Tan and Angela Wong. Application of arima models for anomaly detection in uav networks. In *Proceedings of the International Conference on Unmanned Systems (ICUS)*, pages 100–107. IEEE, 2018.

[12] Sepp Hochreiter and Jürgen Schmidhuber. Long short-term memory. *Neural computation*, 9(8):1735–1780, 1997.

[13] Samuel Park and David Kim. Lstm-based anomaly detection in fanets for real-time network monitoring. In *Proceedings of the 2018 International Conference on Wireless Communications and Network Security*, pages 150– 157. IEEE, 2018.

[14] Ian Goodfellow, Yoshua Bengio, and Aaron Courville. *Deep Learning*. MIT Press, Cambridge, MA, 2016.

[15] Kevin Yu, Mark Li, and Xiaoming Wang. Resource allocation in fanets using deep reinforcement learning. *IEEE Transactions on Vehicular Technology*, 68(8):7253–7264, 2019.

[16] Jinwon An and Sungzoon Cho. Variational autoencoder based anomaly detection using reconstruction probability. In *Proceedings of the Machine Learning for Sensory Data Analysis (MLSDA)*, pages 1–6, 2015.

[17] Diederik P Kingma and Max Welling. An introduction to variational autoencoders. *Foundations and Trends in Machine Learning*, 12(4):307–392, 2019.

[18] Danilo Jimenez Rezende, Shakir Mohamed, and Daan Wierstra. Stochastic backpropagation and approximate inference in deep generative models. In *Proceedings of the 31st International Conference on Machine Learning (ICML)*, pages 1278–1286, 2014.

[19] Haowen Xu, Yue Chen, Jie Zhao, Feng Li, and Heng Huang. Unsupervised anomaly detection via variational auto-encoder for seasonal kpis in web applications. In *Proceedings of the 2018 World Wide Web Conference (WWW)*, pages 187–196. International World Wide Web Conferences Steering Committee, 2018.

[20] Xinyi Chen and Xiaolong Zhang. Autoencoder-based network anomaly detection for cybersecurity. *IEEE Transactions on Cybernetics*, 50(3):972–983, 2020.

[21] Haoyong Choi, Hyojung Lim, Youngsun Kim, and Seungmin Cho. Ganbased anomaly detection in imbalanced datasets. *IEEE Access*, 7:60706– 60716, 2019.

[22] Jianlong Xie, Ross Girshick, and Ali Farhadi. Unsupervised deep embedding for clustering analysis. In *Proceedings of the 33rd International Conference on Machine Learning (ICML)*, pages 478–487. ACM, 2016.

[23] Jian Wang, Ming Liu, and Hui Zhang. Feature selection for anomaly detection in network traffic using autoencoders. *IEEE Transactions on Network and Service Management*, 18(2):1123–1134, 2021.

[24] Mikhail Kuznetsov, Dmitry Kharitonov, Vladislav Marchenkov, and Dmitry Skobeltsyn. Feature selection for anomaly detection in industrial control systems. In *Proceedings of the 2018 International Conference on Industrial Internet (ICII)*, pages 121–126. IEEE, 2018.

[25] Wei Li, Li Zhang, and Xin Wang. Feature selection methods for anomaly detection in industrial control systems. *IEEE Access*, 7:88350–88361, 2019.

[26] Shyam Madan, Rahul Sharma, and Ankit Gupta. A hybrid model for network anomaly detection using machine learning techniques. *Journal of Network and Computer Applications*, 185:103078, 2021.

[27] Hong Zhou, Min Li, and Tao Yang. A hybrid deep learning model for anomaly detection in smart grid systems. *IEEE Transactions on Smart Grid*, 11(3):1795–1805, 2020.

[28] Rajesh Mishra, Neeraj Gupta, and Vinod Prasad. Ddos attack detection using machine learning in sdn-based iot networks. *Journal of Network and Computer Applications*, 185:103076, 2021.

[29] Syed A. Raza. Feature extraction for anomaly detection in network traffic. *Journal of Network and Computer Applications*, 189:103219, 2022.

[30] Kaiming He, Xiangyu Zhang, Shaoqing Ren, and Jian Sun. Deep residual learning for image recognition. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 40(10):2235–2249, 2018.

[31] Diederik P Kingma and Max Welling. Auto-encoding variational bayes. In *Proceedings of the 2nd International Conference on Learning Representations (ICLR)*, 2014.