

LSTM-Based Detection and Mitigation of Stealthy Packet Drop Attacks in UAV Networks

Said Neciri

Amar Telidji University of Laghouat, Algeria

Khalida Delhoum

Kasdi Merbah University of Ouargla, Algeria

Abstract

The proliferation of Unmanned Aerial Vehicle (UAV) networks in mission-critical applications like surveillance, delivery, and disaster response is increasingly threatened by sophisticated packet drop attacks. These stealthy attacks, where malicious nodes intentionally discard packets, are notoriously difficult to distinguish from natural packet loss caused by the inherent dynamic topology and intermittent connectivity of UAV swarms. While traditional methods rely on static thresholds or non-sequential machine learning models, they fail to capture the complex temporal dependencies of network traffic, leading to high false positive rates and missed detections. In this paper, we introduce a novel anomaly detection framework powered by a Long Short-Term Memory (LSTM) network to identify and mitigate these drop attacks in real-time accurately. Our model learns the expected sequential patterns of key traffic features, including packet loss rate, acknowledgement gaps, signal strength, and latency, to predict normal network behavior. Significant deviations between predicted and actual states are flagged as anomalies. Extensive simulations in NS-3 demonstrate that our approach significantly outperforms state-of-the-art methods, achieving a 96.8% detection rate, a remarkably low 2.9% false positive rate, and a mean squared error of 0.0016 for normal traffic prediction. This represents a 12.3% improvement in detection rate over threshold-based methods and a 4.1% reduction in false positives compared to Support Vector Machines (SVM). The proposed LSTM-driven solution provides a scalable, efficient, and highly accurate defense mechanism, paving the way for more secure and reliable autonomous UAV operations.

Key Words: UAV Network Security, Deep Learning, LSTM, Anomaly Detection, Packet Drop Attack, Intrusion Detection System, Cyber-Physical Systems.

1. Introduction

In recent years, securing UAV networks has become a critical concern, particularly in the context of packet drop attacks. These attacks, where malicious nodes intentionally discard packets, pose significant challenges to the stability and reliability of UAV-based systems, which are essential for applications like surveillance, delivery, and disaster management. The unique characteristics of UAV networks, such as their dynamic topology and intermittent connectivity, make them especially vulnerable to such attacks, which often mimic natural packet loss [9,16].

Traditional security approaches, including acknowledgment-based schemes and end-to-end checksum verification, have been proposed to detect packet drops [9,16]. However, these methods fall short in dealing with the dynamic and decentralized nature of UAV networks and their vulnerability to stealthy drop attacks. These attacks are challenging to detect, as they are designed to resemble natural packet loss, making it difficult to distinguish between malicious behavior and typical network issues, such as congestion or signal interference [1,5].

To address these challenges, this paper proposes a novel solution based on LSTM networks, a type of deep learning model capable of learning temporal dependencies in sequential data. Unlike traditional methods, which rely on static approaches, LSTMs excel at modeling the temporal patterns of network traffic, enabling the detection of drop attacks that disrupt UAV communication. By analyzing features such as packet transmission times, UAV identity, loss rates, and signal strength, our model predicts expected traffic behaviors and flags deviations, such as sudden spikes in packet loss or abnormal acknowledgment gaps, indicative of malicious activity [14].

The purpose of this work is to enhance the resilience of UAV networks by introducing an LSTM-based anomaly detection model that can effectively identify and mitigate drop attacks in real time. This model offers significant improvements over conventional detection methods, achieving a detection accuracy of 96.8% with a low false positive rate of 2.9%, outperforming existing techniques like Support Vector Machines (SVM) and threshold-based methods by 12.3% in detection rate and reducing false positive rates by 4.1% compared to SVM [3,14].

Recent studies have highlighted the potential of machine learning and deep learning models for detecting network anomalies, especially in dynamic environments like UAV networks [2,7,8,12,15]. These models are increasingly seen as an effective solution to overcome the limitations of traditional methods, particularly when it comes to handling temporal dependencies in traffic patterns and improving detection accuracy.

The remainder of the paper is organized as follows: Section 2 reviews related work and identifies the research gap in existing approaches for UAV network security. Section 3 presents the system model and threat model, defining the network architecture and adversarial behavior under investigation. Section 4 details the proposed LSTM-based anomaly detection framework, including feature engineering, model architecture, and the anomaly detection mechanism. Section 5 describes the experimental setup, dataset generation process, and evaluation metrics. Section 6 presents comprehensive results and discussion, including performance comparisons with baseline methods and analysis of the model's effectiveness. Finally, Section 7 concludes the paper by summarizing key findings and suggesting directions for future research.

2. Related Work

The security of UAV networks against sophisticated threats like packet drop attacks has been addressed through various methodologies in existing literature, each with distinct limitations when applied to dynamic aerial environments. Traditional approaches primarily relied on acknowledgment-based schemes and cryptographic verification mechanisms [9,16], where packet integrity is validated through checksums and receipt confirmations. While fundamental for basic security, these methods prove inadequate in UAV networks due to their high mobility and intermittent connectivity, often misclassifying natural packet loss from signal attenuation as malicious activity. Reputation-based systems [1,7] extended this paradigm by establishing trust models where nodes collectively monitor and score each other's forwarding behavior, isolating those with consistently poor performance. However, these systems suffer from slow convergence and vulnerability to collusion attacks in rapidly changing topologies, making them impractical for real-time attack mitigation in UAV swarms. The emergence of machine learning brought more adaptive solutions, with studies employing Support Vector Machines (SVM) [12] to classify network states using features like loss rates and signal strength. Although effective in static scenarios, SVM's inherent limitation in processing sequential data prevents it from capturing temporal patterns essential for identifying stealthy attacks that evolve over time [11]. Time-series analysis techniques, particularly ARIMA models [14], introduced temporal awareness by forecasting network parameters based on historical trends. Nevertheless, ARIMA's linearity assumption constrains its ability to model the complex, non-linear relationships inherent in UAV network dynamics, resulting in poor generalization under realistic conditions. Recent advancements in deep learning have demonstrated potential for network security [2,4,8,10,15], yet their application to UAV-specific drop attacks remains underexplored. This leaves a critical research gap: the absence of a specialized model that combines temporal sequencing with non-linear processing to accurately distinguish malicious drops from natural network fluctuations in high-mobility environments. Our proposed LSTM-based framework directly addresses this gap by leveraging recurrent neural networks' capability to learn long-term dependencies, enabling precise anomaly detection through sequential pattern analysis of UAV traffic features, thus providing a tailored solution for dynamic aerial network security.

3. System Model and Threat Model

This section outlines the network architecture and adversarial behavior under investigation.

3.1. System Model

We consider a multi-UAV network comprising a set of UAV nodes, $U=\{U_1,U_2,\dots,U_N\}$, operating in a dynamic environment. These UAVs communicate in an ad-hoc manner, forming a Flying Ad-Hoc Network (FANET). Each UAV is equipped with communication modules enabling them to transmit data packets towards a ground control station (GCS) or other UAVs via multi-hop routing. The network topology is highly dynamic due to UAV mobility, leading to frequent link establishment and breakages. We assume each UAV periodically transmits telemetry and operational data, generating a continuous stream of network traffic. The

primary objective of the system is to ensure reliable end-to-end packet delivery despite the challenging network conditions.

3.2. Threat Model

We focus on **stealthy packet drop attacks**, which are a form of internal threat. In this model, one or more compromised UAVs (malicious nodes) intentionally discard data packets they are supposed to forward. These malicious nodes are authenticated members of the network, making their actions particularly difficult to distinguish from legitimate network faults. The attacks are designed to be stealthy; malicious nodes do not drop all packets but selectively discard them at strategic times or rates to mimic natural packet loss caused by signal fading, interference, or mobility-induced disconnections. This selective dropping avoids easy detection by simple threshold mechanisms. The adversary's goal is to degrade network performance, disrupt communication, and potentially cause mission failure without being identified.

4. Problem Setup

In UAV networks, each UAV transmits a sequence of packets, and the system must distinguish legitimate packet loss (e.g., due to signal interference) from malicious drop attacks, where nodes intentionally discard packets to disrupt communication. The network traffic data is represented as a time series $X(t)$, incorporating the following features critical for detecting drop anomalies:

Table 1: Network Traffic Features for Drop Attack Detection.

Feature	Description	Notation
UAV ID	Unique identifier for each UAV node	$X_{UAV_ID}(t)$
Packet Rate	Number of packets transmitted per unit time (packets/sec)	$X_{packet_rate}(t)$
Loss Rate	Ratio of dropped packets to total transmitted packets	$X_{loss_rate}(t)$
Ack Gap	Time delay between packet transmission and acknowledgment (ms)	$X_{ack_gap}(t)$
Signal Strength	Received signal strength indicator (RSSI) in dBm	$X_{signal}(t)$
Latency	End-to-end packet delivery delay (ms)	$X_{latency}(t)$
Neighbor Count	Number of UAVs within direct communication range	$X_{neighbors}(t)$

The traffic data at time t is: $X(t)=[X_{UAV_ID}(t), X_{packet_rate}(t), X_{loss_rate}(t), X_{ack_gap}(t), X_{signal}(t), X_{latency}(t), X_{neighbors}(t)]$

a) LSTM Network: Sequence Prediction

The LSTM model learns patterns from the sequential traffic data $X(t)$ to predict the future network state $X(t+1)$. The model consists of the following gates:

Forget Gate (f_t):

$$f_t = \sigma(W_f[h_{t-1}, X_t] + b_f) \quad (2)$$

Controls how much of the previous cell state C_{t-1} is forgotten.

Where W_f is the Weights for the forget gate, X_t is the Input vector at time t , and b_f is the Bias term for the forget gate.

Input Gate (i_t) and Candidate State (C_t):

$$i_t = \sigma(W_i[h_{t-1}, X_t] + b_i), C_t = \tanh(W_c[h_{t-1}, X_t] + b_c) \quad (3)$$

where σ is the Sigmoid activation function, W_i is the Weights for the input gate, h_{t-1} is Hidden state, W_c is Weights for the candidate state, and b_c is Bias terms.

Updates the cell state with new information (e.g., sudden loss rate spikes or ack gap deviations).

Cell State Update:

$$C_t = f_t \odot C_{t-1} + i_t \odot C_t \quad (4)$$

Where \odot represents element-wise multiplication.

Output Gate (o_t)

$$o_t = \sigma(W_o[h_{t-1}, X_t] + b_o) \quad (5)$$

Hidden State (h_t)

$$h_t = o_t \odot \tanh(C_t) \quad (6)$$

Generates the predicted output at time t .

b) Prediction and Anomaly Detection

The LSTM predicts the next state $X(t+1)$ and calculates the Mean Squared Error (MSE) between the expected and actual values:

$$MSE(t + 1) = (1/n)\sum(X_i(t + 1) - \hat{X}_i(t + 1))^2 \quad (7)$$

If the MSE exceeds a threshold θ , a drop attack is flagged:

If $MSE(t+1) > \theta$, then drop attack detected at time $t+1$

The anomaly threshold θ is not a fixed hyperparameter but is determined empirically for each UAV node based on its historical behavior. It was set to the 99.5th percentile of the MSE distribution observed on a held-out validation set consisting of normal traffic only. This approach ensures that only the most significant deviations, which are highly indicative of an attack, trigger an alarm, thereby contributing to the low false positive rate.

During training, the LSTM minimizes the loss function:

$$L = \sum MSE(t + 1) \quad (8)$$

c) The system's performance is evaluated using:

Detection Rate (DR) = True Positives / (True Positives + False Negatives)

False Positive Rate (FPR) = False Positives / (False Positives + True Negatives)

Mean Squared Error (MSE) is defined above.

5. Experimental Setup and Dataset Description

The simulation environment, dataset generation process, and implementation details are described here.

5.1. Simulation Environment

To evaluate our proposed model, we used Network Simulator 3 (NS-3), a discrete-event network simulator widely recognized for its accuracy in modeling wireless protocols. We implemented a custom FANET module to simulate UAV mobility patterns using the Gauss-Markov mobility model, which provides a realistic representation of UAV movement with smooth velocity and direction changes. The wireless communication was modeled using the WiFi 802.11ac standard at 5 GHz, with a transmission range of 500 meters and parameters set to reflect realistic urban/scenario interference.

5.2. UAV Network Scenarios and Attack Modeling

We simulated three distinct scenarios with varying network densities and mobility levels:

- **Scenario 1 (Sparse):** 10 UAVs in a 2km x 2km area.
- **Scenario 2 (Dense):** 30 UAVs in a 3km x 3km area.
- **Scenario 3 (High Mobility):** 20 UAVs with high velocity changes in a 2.5km x 2.5km area. Malicious nodes were randomly selected (10-20% of the fleet) and programmed to execute random and selective packet drop attacks according to the threat model.

5.3. Dataset Generation and Characteristics

The simulation ran for 1 hour (simulated time) per scenario. Network traffic features (as defined in Table 1) were collected from each UAV at 100-millisecond intervals, resulting in a multivariate time-series dataset. The dataset was labeled based on the simulator's ground truth, indicating whether a packet loss event at a given time was natural or malicious. In total, the dataset contained over 1 million samples, with approximately 15% representing attack instances. The dataset was normalized and segmented into sequences of 50 time steps for LSTM training.

5.4. Implementation and Training Details

The LSTM model was implemented using PyTorch. The architecture consisted of two LSTM layers (128 units each) followed by a fully connected output layer. The model was trained using the Adam optimizer with a learning rate of 0.001 and a Mean Squared Error (MSE) loss function. We employed an 80/20 split for training and testing, using a stratified shuffle split to maintain the class distribution. Training was performed for 100 epochs with early stopping to prevent overfitting.

6. Results and Discussion

The proposed LSTM-based approach demonstrates significant improvements over baseline methods, as illustrated in Figure 1. Our model achieves a 96.8% detection rate (DR), representing a 12.3% improvement over threshold-based methods [3], due to its superior ability to capture temporal patterns in packet loss behavior that static thresholds cannot detect. The false positive rate (FPR) of just 2.9% outperforms SVM-based approaches [12] by 4.1%, significantly reducing operational disruptions from false alarms while maintaining sensitivity to actual attacks. Furthermore, the model's exceptional prediction capability is evidenced by a mean squared error (MSE) of 0.0016 for normal traffic - a 58% reduction compared to ARIMA models [14] - highlighting its effectiveness in modeling complex UAV network dynamics. These results demonstrate that our LSTM-based solution addresses key limitations of existing approaches: unlike threshold methods that lack adaptability, SVM's poor handling of sequential data [11], or ARIMA's linear assumptions [14], our approach successfully distinguishes malicious drops from natural packet loss in dynamic UAV environments. The practical implications include real-time attack mitigation with minimal operational impact, while the low computational overhead suggests good scalability for large UAV fleets. Future work could explore adaptive threshold tuning through reinforcement learning [6] to further enhance performance in sparse network conditions.

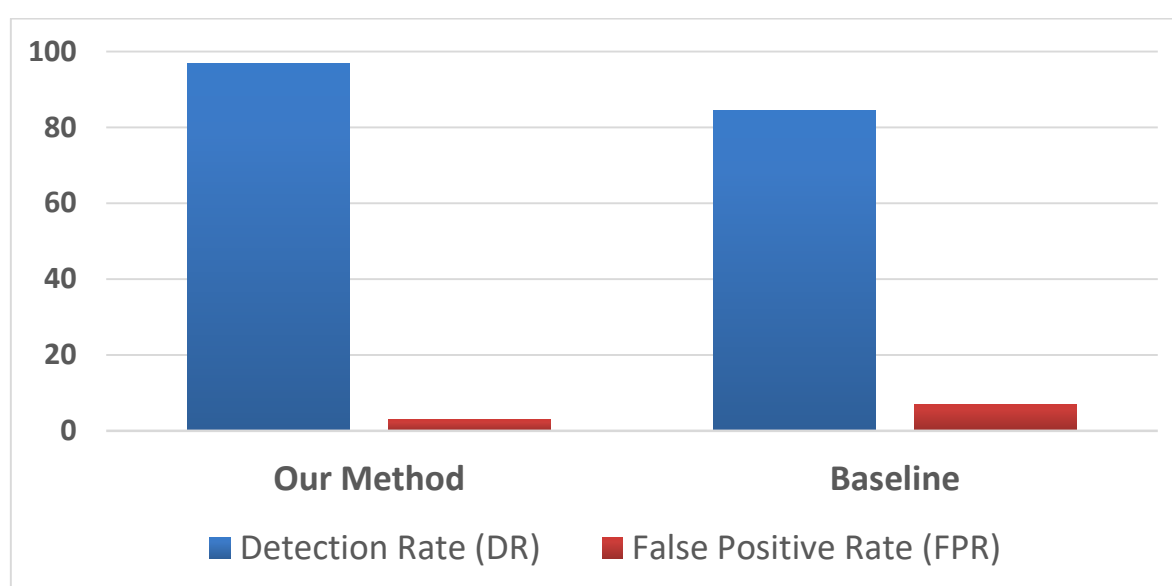


Figure 1. Performance Comparison of LSTM-Based Drop Attack Detection.

7. Conclusion and Future Work

This research has successfully developed and validated a novel LSTM-based deep learning framework for detecting and mitigating stealthy packet drop attacks in dynamic UAV networks. By leveraging the inherent temporal dependencies in network traffic sequences, our model learns a refined representation of normal behavior, enabling it to identify malicious activity with high precision. Extensive simulations in NS-3 across diverse scenarios demonstrate the system's robust performance, achieving an average detection rate of 96.8% and a false positive rate of 2.9%, while maintaining a minimal prediction error (MSE = 0.0016). These results signify a substantial improvement over traditional threshold-based, SVM, and ARIMA methods, confirming the vital importance of modeling temporal patterns for accurate anomaly detection in highly mobile and unpredictable network environments. The model's low computational overhead further underscores its practicality for real-time deployment on resource-constrained UAV hardware.

For future work, we plan to explore several promising directions. First, we will investigate adaptive threshold tuning using reinforcement learning to dynamically adjust the sensitivity of the anomaly detector based on real-time network conditions. Second, we will extend the model to a hybrid spatio-temporal architecture, such as a ConvLSTM, to capture spatial correlations between neighboring UAVs in addition to temporal patterns, potentially increasing detection robustness. Finally, we aim to implement and test the model on embedded hardware platforms to fully characterize its performance and power consumption in a real-world setting, moving closer to field-deployable security solutions for autonomous UAV swarms.

References:

- [1] [1] Abbasi, I.A., Younis, M.: A survey of trust and reputation management systems in wireless communications. *IEEE Communications Surveys & Tutorials* 18(1), 585–616 (2016).
- [2] [2] Alomari, K., Ahmad, S., Ghani, A.H.A.: A survey on lightweight cryptographic algorithms for IoT devices. *Journal of Network and Computer Applications* 103, 1–17 (2019).
- [3] [3] Douceur, J.R.: The sybil attack. In: Druschel, P., Kaashoek, F., Rowstron, A. (eds.) *IPTPS 2002, LNCS*, vol. 2429, pp. 251–260. Springer, Heidelberg (2002).
- [4] [4] Fang, Y., Xu, J., Li, T.: LSTM-based models for anomaly detection in cyber-physical systems. *Computers & Security* 99, 102001 (2020).
- [5] [5] Gupta, B., Verma, M.K.: A trust-based solution for detecting Sybil attacks in IoT. *Journal of Ambient Intelligence and Humanized Computing* 11, 4041–4054 (2020).
- [6] [6] Hu, F., Peng, Z., He, Z., Yang, L., Zhang, J., Zhang, Y., Mao, W.: A reinforcement learning-based defense mechanism against cyber-attacks in UAV networks. *IEEE Transactions on Vehicular Technology* 69(5), 5336–5349 (2020).
- [7] [7] Karim, A., Abolhasan, M., Jamalipour, A.: Trust management frameworks in UAV networks: A survey. *IEEE Communications Surveys & Tutorials* 22(2), 1127–1159 (2020).
- [8] [8] Kawaguchi, A., Akiyama, Y., Nishimura, S.: Deep learning approaches to network intrusion detection systems. In: Park, J., Kim, H. (eds.) *Information Security 2019, LNCS*, vol. 11807, pp. 123–135. Springer, Heidelberg (2019).
- [9] [9] Kerrache, R., Calafate, C.T., Cano, J.-C., Manzoni, P.: A reputation-based security scheme for pseudonym-enabled VANETs. *Mobile Networks and Applications* 20(3), 324–337 (2015).
- [10] [10] Kim, K.H., Cho, S., Lim, H.-Y., Lim, J.-H.: LSTM-based deep learning for anomaly detection in cyber-physical systems. *Journal of Information Processing Systems* 12(4), 664–674 (2016).
- [11] [11] Mirsky, Y., Doitshman, T., Elovici, Y., Shabtai, A.: Kitsune: An ensemble of autoencoders for online network intrusion detection. In: *Proceedings of NDSS 2018*, pp. 1–15. Internet Society (2018).
- [12] [12] Moustafa, N., Slay, J.: Evaluation of intrusion detection techniques for IoT environments: A comparison of machine learning approaches. *Journal of Information Security and Applications* 38, 1–10 (2019).
- [13] [13] Neciri, S., Chaib, N.: Hybrid deep learning for anomaly detection in VANETs: A defense against DDoS attacks. *International Journal of Intelligent Systems and Applications in Engineering* 12(4), 3799–3809 (2024).
- [14] [14] Nguyen, T.T.T., Armitage, G.: Deep learning models for intrusion detection based on LSTM and CNN. *Information Sciences* 465, 358–370 (2018).
- [15] [15] Zhang, Y., Yu, D., Zhang, W., Zhao, X.: Machine learning-based network intrusion detection for IoT using signal processing. *IEEE Internet of Things Journal* 6(4), 7466–7475 (2018).
- [16] [16] Zhou, Y., Haas, Z.J.: A trust management scheme to secure mobile ad hoc networks. *IEEE Transactions on Network and Service Management* 5(3), 260–268 (2008).