AI-based Approach for Radio Frequency Jamming Attack Detection in Unmanned Aerial Vehicles

Jetani Harshil, Harikrushna Goti
Department of Comp. Sci. & Engg.
Institute of Technology,
Nirma University, Ahmedabad, India
{23bce515, 23bce513}@nirmauni.ac.in

Nikunjkumar Mahida
Department of Comp. Sci. & Engg.
Institute of Technology,
Nirma University, Ahmedabad, India
21bce166@nirmauni.ac.in

Rajesh Gupta
Department of Comp. Sci. & Engg.
Institute of Technology,
Nirma University, Ahmedabad, India
rajesh.gupta@nirmauni.ac.in

Sudeep Tanwar
Department of Comp. Sci. & Engg.
Institute of Technology,
Nirma University, Ahmedabad, India
sudeep.tanwar@nirmauni.ac.in

Geetika Bhardwaj
Department of Comp. Sci. & Engg.
Guru Nanak Dev Engineering College
Ludhiana, Punjab, India
inbox.geetika@gmail.com

N.Z Jhanjhi, Sayan Kumar Ray*
School of Computer Science
Taylor's University
Subang Jaya, Malaysia
{noorzaman.jhanjhi, sayan.ray}@taylors.edu.my
**Corresponding Author*

***Abstract*—Unmanned Aerial Vehicles (UAV) are highly versatile systems with applications expanding in various fields, for instance, Surveillance, Reconnaissance, Disaster Response, Agriculture, and many more. Although UAVs have many important advantages over conventional manned aircraft, such as cheaper operating costs and a lower risk for human pilots, their vulnerability to Radio Frequency (RF)-jamming poses a substantial risk to navigation and communication systems by disrupting signals. UAVs depend on remote control and autonomous operations. These attacks are concerning in many application areas. Communication and navigation play crucial roles in these autonomous systems. This paper aims to explore different deep-learning algorithms for the detection of RF-jamming attacks in UAVs. A comparison analysis is conducted to evaluate five distinct architectures using conventional evaluation metrics criteria comprising accuracy, precision, recall, confusion matrices, and the area under the ROC curve. These comparative analyses helped in selecting an accurate architecture for the definition, RNN architecture gave an impressive accuracy of 93% and demonstrated a superior performance than other architectures. This paper aims to strengthen RF-jamming detection systems in UAVs to enhance their safety and operational reliability in several scenarios.**

***Index Terms*—Deep learning, RNN, RF-jamming, UAVs, VANETs**

I. Introduction

UAVs have become increasingly indispensable across different industries, although initially it was developed for military purposes, nowadays they are used in many applications. In agriculture, UAVs enable precision farming, which allows farmers to monitor crops, assess land conditions, and apply fertilizers or pesticides with great accuracy. It increases agricultural productivity, minimizes environmental impact, and helps to reduce resource usage. In disaster management, UAVs are vital in search and rescue operations, air supervision, mapping affected areas, and supplying to offensive places. With the current advancements in technology and regulatory framework, UAVs have unlocked new possibilities and emerged in various domains.

With an emphasis on ad hoc mobile communication between cars and infrastructure, initially, VANETs were designed to provide networks for creating and relaying information between vehicles. VANETs can, however, be the target of jamming attacks, which might interfere with transmission frequencies and potentially have unfavorable effects. Wireless communications are seriously threatened by intentional or accidental RF interference, with jamming being a popular attack technique. These attacks can increase the risk of accidents, disrupt automated driving systems, and impede the transmission of critical information, such as traffic updates and collision alerts[1]. It is crucial to categorize RF-jamming occurrences to differentiate between deliberate and accidental interference by considering factors like speed, timing, SNR, and RSSI. Textual data acquired from these factors allows for effective classification of jamming occurrences utilizing DL techniques like Hybrid RNN and LSTM models. This classification is especially useful in urban settings where communication issues are higher and there is a lack of adequate communication infrastructure, such as urban highways with few available towers[2].

Classification of attacks on UAVs is mandatory for improving protection strategies, enabling adaptive responses like altering flight paths or activating fail-safe modes upon detection. Swift communication of attack information to ground control facilitates is imperative for informed decision-making, allowing operators to include appropriate countermeasures or re-route the UAVs. By analyzing attack patterns that filter security protocols, proactive measures for preventing future incidents are implemented. Integrating encryption and data protection safeguards ensures the integrity and confidentiality of transmitted data. By leveraging classification techniques, UAV protection strategies can be strengthened, ensuring safe and reliable operation in diverse environments.

Realizing the potential of AI techniques, several researchers have focused on incorporating this methodology into the field of RF-jamming detection in an effective manner. Various strategies are employed by researchers for the effective use of ML's potential in this field. Well-known research by Pace *et al.* adopted an approach based on machine learning methods, such as Decision trees and Multi-layer perceptrons [3] with