Pervasive Intrusion Detection Scheme to Mitigate Sensor Attacks on UAV Networks

Simeon Okechukwu Ajakwe, Vivian Ukamaka Ihekoronye, Dong-Seong Kim, and Jae Min Lee

IT Convergence Engineering, Kumoh National Institute of Technology Gumi, South Korea
(simeonajlove, ihekoronyevivian)@gmail.com, (ljmpaul, dskim)@kumoh.ac.kr

Abstract—A secured drone transportation system requires a ubiquitous approach to detecting and preventing attacks on UAV operations in the airspace. This study proposed a novel pervasive intrusion detection scheme (PIDS) for achieving this using recurrent neural networks. The dataset comprises normal and malicious (jamming and spoofing) flight logs from 6 UAV models. Performance evaluation is carried out on different one-class classifiers. The simulation shows that OC-AE achieved a superior 92% precision, 99% sensitivity, and 96% F1-score detection than other classifiers across all the UAV platforms.

Index Terms—Drone transportation, Deep Learning, Intrusion Detection, Internet of Drones, UAV, Sensor

I. INTRODUCTION

The security of unmanned aerial vehicles (UAV) drone for conveying goods and services, also known as drone transportation systems (DTS) is a critical issue in advancing this emerging innovation [1]. Generally, attacks on drones aim at diverting such aircraft from reaching their defined destination. These attacks target the communication network signal reception between the drone and its ground control station (GCS). Identifying and preventing an unforeseen and pre-mediated attack on a UAV network is an unavoidable technical issue [2]. UAV network attacks come in the form of jamming or spoofing attacks. An intrusion detection system (IDS) identifies an ongoing attack on a network. Conversely, an intrusion prevention system (IPS) prevents the occurrence of attacks. IDS can be statistical-based, specification-based, signature-based, anomaly-based, or hybrid. The objective of an IDS/PIS design is efficient and effective intrusive behavior classification.

Intrusion detection in UAV networks is a complicated task. The dynamic threat landscape of UAVs due to technological progress makes signature-based IDS detection incapable of protecting the UAV networks effectively against threats. Also, different UAV platforms come with diverse configurations making existing solutions incapable. With the increase in the frequency of attacks on UAV networks, it becomes imperative to develop an interoperable and pervasive approach. IDS task as a classification problem can be either binary (normal or abnormal network traffic behavior) or multi-class (different types of abnormal network traffic behavior). The traditional method, machine learning (ML), or deep learning (DL) approach is used to achieve this objective. As data feature complexity increases, DL models have a high capacity to extract better representations from such data than ML classifiers.

Popular attempts to handle IDS issues in the UAV domain include LSTM-based anomaly detection by authors [3]. However, due to the heterogeneity of UAV control configurations, sensors, communication protocols, etc. in response to 6G [4], none of these approaches can sufficiently tackle intrusion detection on UAV sensor networks as it requires varieties of datasets. Hence, the need for a method that can adequately accommodate these characterizations.

Unlike anomaly detection, pervasive intrusion detection (PIDS) comes with the ability to learn from a training dataset without anomalies. It allows the PID to utilize the existing flight logs of UAV sensors to learn what is normal for the specific UAV to be operated on by the IDS. Hence, the proposed approach distinguishes messages as either known or attacks by learning from normal UAV sensor signal behavior. This study leverages the capabilities of artificial intelligence models, especially autoencoders, an unsupervised DL recurrent neural network (RNN) model to address this problem efficiently. Its novelty is to demonstrate the use of one-class classifiers (OCC) to solve sensor attack problems in UAV platforms with different specifications. In this paper, section II explores the OCC framework and dataset description, section III discusses the results and performance evaluation, and section IV concludes the paper with a promising direction.

II. METHODOLOGY

OCC framework is an artificial intelligence classification approach that detects abnormal data points from a given imbalanced dataset and compares it with normal (known) class instances. OCC approach includes a support vector machine (OC-SVM), Isolation Forest (OC-IF), local outliers (LOF), and autoencoders (OC-AE). In this context, flight logs from the training flight of UAV sensor records used to conduct an operation constitute the known class. A variation from the normal is considered abnormal. This study covers OC-SVM, LOF, and OC-AE approaches.

Fig. 1 shows succinctly the adopted approach in this study in ascertaining whether an incoming signal in a UAV network is an intrusion or not, depending on the underlying detection and classification algorithm. Each classifier is subjected to different analyses based on its unique characteristics.

The dataset used is available on IEEE Dataport [5]. It comprises normal (benign) and abnormal (malicious) records with multiple attributes created from an experimental setup involving 6 UAV models. The abnormal records are jamming and spoofing attacks. To eliminate unuseful features, feature
clustering was performed. We applied principal component analysis for dimensionality reduction. The simulation platform is in a Python environment with Windows 10 operating system.

III. RESULT DISCUSSION AND PERFORMANCE EVALUATION

The results in Table I shows the performance of the OC-AE model across the 6 UAV models using precision, sensitivity, and F1-score. F1-score measures the rationality in behaviour of a model which is a function of the change in precision and sensitivity values; in the course of carrying its operation expressed as:

$$F_1^{score} = \frac{1}{\Delta(P_r \times R_c) \times \Delta(P_r + R_c)}$$

TABLE I INTRUSION DETECTION BY AUTOENCODER

<table>
<thead>
<tr>
<th>UAV Platforms</th>
<th>Attacks</th>
<th>OC-SVM</th>
<th>AUTOENCODER</th>
<th>LOF</th>
</tr>
</thead>
<tbody>
<tr>
<td>DeltaQuad VTOL</td>
<td>Malicious</td>
<td>0.58</td>
<td>0.99</td>
<td>0.55</td>
</tr>
<tr>
<td></td>
<td>Benign</td>
<td>0.96</td>
<td>0.99</td>
<td>0.94</td>
</tr>
<tr>
<td>Holybro S500</td>
<td>Malicious</td>
<td>0.81</td>
<td>0.99</td>
<td>0.83</td>
</tr>
<tr>
<td></td>
<td>Benign</td>
<td>0.99</td>
<td>0.99</td>
<td>0.73</td>
</tr>
<tr>
<td>Standard Plane</td>
<td>Malicious</td>
<td>0.41</td>
<td>0.95</td>
<td>0.35</td>
</tr>
<tr>
<td></td>
<td>Benign</td>
<td>0.93</td>
<td>0.99</td>
<td>0.91</td>
</tr>
<tr>
<td>Standard Tailsitter</td>
<td>Malicious</td>
<td>0.72</td>
<td>0.95</td>
<td>0.65</td>
</tr>
<tr>
<td></td>
<td>Benign</td>
<td>0.98</td>
<td>0.99</td>
<td>0.97</td>
</tr>
<tr>
<td>Yuneec H480</td>
<td>Malicious</td>
<td>0.68</td>
<td>0.93</td>
<td>0.18</td>
</tr>
<tr>
<td></td>
<td>Benign</td>
<td>0.99</td>
<td>0.99</td>
<td>0.89</td>
</tr>
<tr>
<td>3DR Iris+</td>
<td>Malicious</td>
<td>0.77</td>
<td>0.90</td>
<td>0.091</td>
</tr>
<tr>
<td></td>
<td>Benign</td>
<td>0.99</td>
<td>0.99</td>
<td>0.73</td>
</tr>
</tbody>
</table>

Average value: 0.82 0.96 0.59

On average, the AE-OC achieved a 92% precision, 99% sensitivity, and 96% F1-score value in differentiating a normal sensor value from a spoofed or jammed value. This implies that OC-AE can adequately detect and prevent UAV sensor attacks.

The results in Table II is a succinct presentation of the performance evaluation. From Figure 2, the average F1-score of LOF is 59%, 82% for OC-SVM, and OC-AE is 96%. These results evidently proves that the deployment of a denoising OC-AE as the underlying detection model in a UAV-IDS, a spoofed or jammed sensor signal on various UAV networks can be significantly detected and averted.

IV. CONCLUSION

This study proposed a novel PIDS for detecting sensor attacks on UAV networks across different configurations using recurrent neural networks. The result shows that denosing autoencoder can adequately detect an attack on UAV sensor.

In the future, the model will be explored for onboard UAV sensor configuration.

ACKNOWLEDGMENT

This research work was supported by Priority Research Centers Program through NRF funded by MEST (2018R1A6A1A03024003) and the Grand Information Technology Research Center support program (IITP-2022-0-01612) supervised by the IITP by MSIT, Korea.

REFERENCES