Supervised Deep Learning Models for Detecting GPS Spoofing Attacks on Unmanned Aerial Vehicles

Tala Talaei Khoei[1], Ghilas Aissou [1], Khair Al Shamaileh[2], Vijaya Kumar Devabhaktuni[3], and Naima Kaabouch[1]

[1]School of Electrical Engineering and Computer Science, University of North Dakota, Grand Forks 58202, ND, USA
[2]Electrical and Computer Engineering Department, Purdue University Northwest, Hammond 46323, IN, USA
[3]Electrical and Computer Engineering Department, The University of Maine, Orono 04469, ME, USA

***Abstract*- Unmanned Aerial Networks (UAVs) are prone to several cyber-atttacks, including Global Positioining Spoofing attacks. For this purpose, numerous studies have been conducted to detect, classify, and mitigate these attacks, using Artificial Intelligence technqiues; howver, most of these studies provided techniques with low detection, high misdetection, and high bias rates. To fill this gap, in this paper, we propose three supervised deep learning techniques, namely Deep Neural Network, U Neural Network, and Long Short Term Memory. These models are evaluated in terms of Accuracy, Detection Rate, Misdetection Rate, False Alarm Rate, Training Time per Sample, Prediction Time, and Memory Size. The simulation results indicated that the U Neural Network outperforms other models with accuracy of 98.80%, a probability of detection of 98.85%, a misdetection of 1.15%, a false alarm of 1.8%, a training time per sample of 0.22 seconds, a prediction time of 0.2 seconds, and a memory size of 199.87 MiB. In addition, these results depicted that the Long Short Term Memory model provides the lowest performance among other models for detecting these attacks on UAVs.**

Keywords— Artificial intelligence, deep learning deep neural network, global positioning system, long short-term memory, machine learning, supervised learning, unmanned aerial network, U-neural network.

I. INTRODUCTION

Unmanned Aerial Vehicles (UAVs) navigation and localization have been active research topics over the past decade. One of the most popular and widely used technologies is the Global Positioning System (GPS), which is suitable for the outdoor environment. In addition, GPS is relatively inexpensive, easy to deploy, and accurate compared to other localization technologies [1]. In light of GPS's widespread use in sensitive applications, such as UAVs and the fact that GPS signals are unencrypted and open to the public, cyber-criminals are targeting GPS receivers using jamming and spoofing attacks.

As a result of a jamming attack, the UAV may lose access to the GPS link, resulting in being forced to turn to alternative but temporary localization techniques, such as vision-based localization or return to home technique [2]. A GPS spoofing attack, on the other hand, sends erroneous and fake GPS signals to a target's receiver without alarming it, resulting in the hijacking or crash of the UAV depending on the complexity of the attack [3].

Artificial intelligence (AI) has been discovered to be a great candidate for detecting cyber-attacks in a heterogeneous and unpredictable environment [2, 3, 4, 5]. AI techniques can efficiently and quickly find hidden patterns in massive volumes of data, making them ideal for large and complex networks. AI-based detection techniques can be costly in terms of training and deployment. In addition, their computational power and memory needs should be assessed, particularly in systems with limited size, weight, and power (SWaP), such as UAV [6, 7]. Therefore, it is important to consider the training cost and the deployment of the models on UAVs.

Several studies proposed machine learning-based (ML) and deep learning-based (DL) detection techniques to detect and classify GPS spoofing attacks. For instance, the authors of [8] proposed two dynamic ML-based models, namely Metric Optimized Dynamic selector and Weighted Metric Optimized Dynamic selector to detect GPS spoofing attacks on UAVs. In this study, the authors developed a one-stage ensemble method to identify the feature importance and correlated features from the dataset and train the data using ensemble selectors.

In [9], the authors focused on tree-based ML models, specifically Random Forest, Gradient Boost, Extreme Gradient Boosting, and Light Gradient Boosting to detect these attacks. In another work [10], the authors compared the performance of instance-based ML techniques, including K-nearest neighbor, Radius Neighbor, Linear Support Vector Machine, C- Support Vector Machine, and Nu- Support Vector Machine. In both works, the authors used confusion matrix-based metrics such as accuracy, probability of detection, false alarm, and probability of misdetection. The evaluation also included memory and processing time requirements.

The authors of [11] used the variations in the fundamental frequency of the GPS signal as input features of different ML models. The extracted features are jitter and shimmer based along with the frequency modulation. The authors performed a K-fold analysis on the selected models. Results showed that the SVM model with a polynomial kernel function is the best-performing model. Despite the acceptable results these techniques showed, they still suffer from some critical limitations, such as high bias rates, overfitting, low detection rates, and difficulty interpreting the results. Therefore, a holistic solution is needed to easily interpret the results and

deal with overfitting issues. For this purpose, DL techniques have been proposed to provide acceptable results, and reduce the bias rate, and overfitting issues.

To address the concerns raised above, numerous studies in the literature investigate the performance of DL models in detecting cyberattacks in different cyber-physical systems [3]. To this end, few works have focused on GPS spoofing detection using DL models. For instance, the authors of [12] proposed a GPS replay attack detection method based on a supervised DL model, namely ANN. In this study, the authors showed the effect of several extracted features from the received signal on detection performance. The best results were obtained by combining five parameters, namely satellite vehicle number, pseudo-range, carrier phase, Doppler shift, and signal-to-noise ratio. In [13], the authors retrieved three signal properties as input features of a supervised DL model, namely a multi-layer neural network. These three input features are early-late phase, delta, and signal level. The proposed method has been evaluated using software-based GPS simulators.

In [14], the authors proposed another supervised DL model, namely LSTM that monitors the derived PVT information from the GPS signal using this DL model. In [15], the authors used a supervised CNN-based model, namely Residual Neural Network to detect GPS spoofing attacks, using the satellite imagery matching approach. The DL-based detection techniques discussed above have shown an improvement in performance compared to ML-based detection techniques, especially in terms of decreasing the false alarm rate. However, they still suffer from a high misdetection rate. This can be due to a variety of reasons, such as the complexity of the detection task, the quality and quantity of the training data, and the specific architecture and hyperparameters of the DL models.

In this paper, DL-supervised learning models are classified into three classes, Artificial Neural Network (ANN), Convolutional Neural Network (CNN), and Recurrent Neural Network (RNN)-based models. From each of the categories, these models are selected: Deep Neural Network (DNN), U Neural Network (U-Net), and Long Short-Term Memory (LSTM) to train, test, and validate the given data, respectively. In addition, we evaluated the models in terms of Accuracy, Detection Rate, Misdetection Rate, and False Alarm Rate. The paper also adds the Training Time per Sample, Prediction Time, and Memory Size to the evaluation criteria to address the issue of SWaP consideration. In short, the important contributions of this paper are summarized as follows:

- Introducing a classification of supervised DL models,
- Developing three supervised DL models, namely DNN, U-Net, and LSTM to detect and classify GPS spoofing attacks on UAVs,
- Providing a comprehensive comparison of these models in terms of Accuracy, Detection Rate, Misdetection Rate, False Alarm Rate, Training Time per Sample, Prediction Time, and Memory Size,
- Studying, comparing, and discussing the result of this study with other studies in literature.

This paper's remainder is organized as follows: Section II discusses the materials used in this study. Section III highlights the results, while Section IV outlines the conclusion.

II. Materials

The corresponding dataset used for training and testing the DL models, described in [9], is briefly reviewed in this section, followed by a discussion of the data pre-processing techniques, classification models, and evaluation metrics used in this work.

A. Dataset

The dataset used in this work was developed and generated by the authors of [9]. The dataset, as shown in Table I, has 13 extracted features from three different GPS receiver stages. Table I depicts the abbreviations of the features along with their brief explanations. The dataset contains three simulated GPS spoofed attacks, namely simplistic, intermediate, and sophisticated attacks. The dataset also includes normal GPS signals collected using a software-defined radio in different scenarios. A binary class consisting of GPS spoofing attacks and normal GPS signal instances is considered for training, testing, and validating the results to offer accurate predictions and easy interpretation. It is worth mentioning that the used dataset consists of 14000 samples, including 7000 attacks and 7000 normal traffic samples.

TABLE I. LISTS OF THE FEATURES IN THE CORRESPONDING DATASET.

Feature	Abbreviations	Descriptions
Satellite Vehicle Number	PRN	Unique identification number of the satellite
The Carrier Doppler	DO	The Carrier Doppler is the result of the satellite and receiver motion. It is expressed as a frequency drift
Pseudo-Range	PD	It refers to the distance between the satellite and the receiver. It is calculated as the difference between transmission and reception time.
Receiver Time	RX	It is the receiver time given in seconds after the start of time of the week.
Time of the week	TOW	The time elapsed in seconds since the start of the week given by the satellite clock
Carrier Phase Cycles	CP	It is the beat frequency drift between the satellite signal and the receiver generated carrier.
Early Correlator	EC	It is at half chip spacing before prompt correlator
Late Correlator	LC	It is at half chip spacing after prompt correlator
Prompt Correlator	PC	The measurement made during coarse acquisition code tracking.
Prompt in phase correlator	PIP	It is the in-phase component of PC
Prompt Quadrature	PQP	It is the quadrotor component of PC

Tacking Carrier Doppler	TCD	It refers to the continuous estimate of the carrier doppler at the tracking loop
Carrier to noise Ratio	C/N_0	The ratio of the received carrier strength and the noise

B. Data Pre-processing

In this study, the data pre-processing step refers to the necessary techniques performed before training the models on the corresponding data. There has been some discussion about how GPS redundancy could affect the performance of AI models [16]. For this reason, it is important to identify the correlated features that need to be discarded from the dataset. According to the results in [9], two features, RX and TCD, which are substantially correlated with TOW and CP, respectively, are removed. As a result, the remaining 11 features, namely PRN, DO, PD, TOW, CP, EC, LC, PC, PIP, PQP, and C/N0, are considered for model training, testing, and validation.

The second step of data pre-processing is data imputation. In this stage, missing values are imputed to the corresponding data. In this work, mode imputation is employed, which replaces the missing value with the highest frequency. Finally, in the third step, data normalization is performed using the Min-Max Scalers, which subtracts the minimum value (excluding the outliers) in the feature and divides it by its range. It is worth mentioning that the given data was balanced, hence, no technique was required to balance the classes [17-19].

C. Classification Models

Fig. 1 provides a schematic overview of the supervised DL models along with their categories. As one can observe, the supervised DL models are classified into three categories, namely Artificial Neural Network (ANN), Convolutional-Neural Network (CNN), and Recurrent Neural Network (RNN)-based models. A short description of these models is provided as follows:

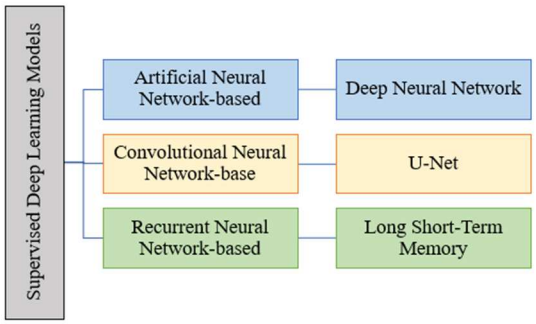


Fig. 1. Classification of Supervised Deep Learning Models.

C.1.Artificial Neural Network

One of the most well-known DL approaches is ANN-based models. These DL models consist of multiple processing elements, namely inputs, and outputs that perform based on the pre-defined activation functions, which makes them simple and efficient. Although their learning process is quite sluggish, DL models in this category often yield good detection rates. In this study, a DNN model is applied as a candidate in ANN-based models to train, test, and validate the results. In general, the DNN consists of an input layer, followed by *N* hidden layers, and an output layer. A simple architecture of this model is presented in Fig. 2. The model has a value in the input layer equal to the number of features in the given dataset. The hidden layers, which are located between the input and output layers, perform based on a weight function. This function exploits the weights of inputs and directs them via an activation function to the output.

DNN models usually have more than two hidden layers (i.e. $N>2$). The output layer shows the number of classes. In addition, an important motivation of DNN models is the trade-off between accuracy and the complexity in their designs This suggests that employing a DNN model with more hidden layers can increase computational complexity, testing and training time, and rate of convergence [20].

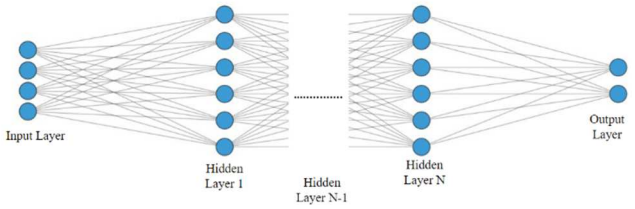


Fig. 2. Architecture of a Deep Neural Network Model.

C.2. U Neural Network

CNN-based models are another type of supervised DL. These models are commonly used to learn feature spatial hierarchies using a backpropagation approach. CNN-based models include Residual Neural Networks, Densely Connected Neural Networks, Alex Neural Networks, Le-Neural Networks, and more. Yet, despite their high performance, these models have several drawbacks, such as requiring massive quantities of data, complex architecture, and reduced computing efficiency.

As a result, a new sort of CNN model, known as the U-Neural Network (U-Net), has been suggested to address these problems. The u-Net architecture was modified and improved so that it could perform with fewer samples, resulting in more accurate classification and segmentation. This model's U-shape design is divided into two halves, as seen in Fig. 3, Analysis Path (Encoder) and Synthesis Path (Decoder).

The encoder architecture is composed of numerous convolutions, followed by Rectified Linear Unit (ReLu) and batch normalization. The Maxpool function minimizes the spatial dimension while increasing the number of feature channels and cutting the spatial dimension in half during the

down sampling phase (Conv + ReLu). The encoder is followed by the decoder, which consists of an up-sampling stage for the feature map, followed by a convolution layer (UpConv). The convolution layers, typically followed by the ReLu function (Conv + ReLu), can minimize the number of features by half. Another convolution is used, along with the SoftMax function, at the last layer to map the channels into the required number of classes, as shown in Fig. 4. Summation (also known as Skip connection) can be used to prevent data loss. In fact, without Summation, data loss may occur from one layer to another layer. This function performs as a bridge between Encoder and Decoder and can be used as an effective tool to recover the details of the output class [21].

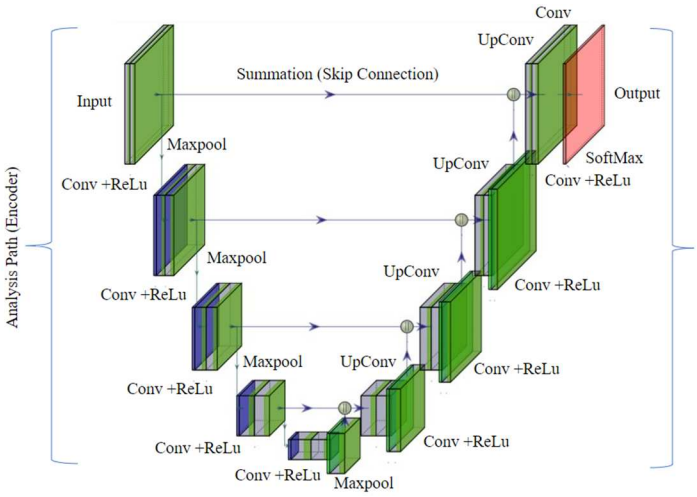


Fig. 3. Architecture of U-Net.

C.3. Long Short-Term Memory

RNN-based models belong to the supervised DL category with chain-like topologies of repeating modules (known as cells), and the cells are utilized as memory to retain essential data from previous processing stages. The LSTM model is a subset of RNN-based models that incorporate interaction per cell to learn long-term dependencies and memorize data over time. The architecture of this model consists of several blocks (or cells) as shown in figure 4. The cell state and the hidden layer are both transferred to the next cell in LSTM. The cell state is considered to be the main chain of data flow, allowing the data to move forward unchanged.

In this context, the data can be added or removed from the cell state through sigmoid gates. In the hidden layer, the input weights are applied and directed to the output layer via the Sigmoid function. The gates are mostly the same as a layer or series of matrix operations, which has multiple individual weights [17]. The LSTM model is designed to prevent long-term dependency problems since it uses some cells as the controlling tool for memorizing procedures. The initial step in building LSTM is to detect unimportant data and remove it from the cell in that step.

The Sigmoid function is mainly responsible for this procedure, taking the output of the last LSTM unit (h_{t-1}) at the time *t-1* and the current input *X* at time *t*. The Sigmoid function also decides the parts that are removed from the old output. In addition, the forget gate, *f,* is a vector ranging from 0 to 1, associated with the number of the cell state, (C_{t-1}). The Sigmoid layer is responsible for the new data that is updated or ignored, whereas the Tanh layer provides a weight to the values which they passed and indicates their level of importance. These values are multiplied to update the new cell state. Then, the new memory is summed up with the old memory, resulting in C_t. In the end, the output can be computed based on the output cell state. Therefore, a Sigmoid layer decides the part of the cell state that makes it to the output, while the output of the Sigmoid gate is multiplied by the new data by the Tanh layer from the cell state with a ranging value between –1 and 1 [22].

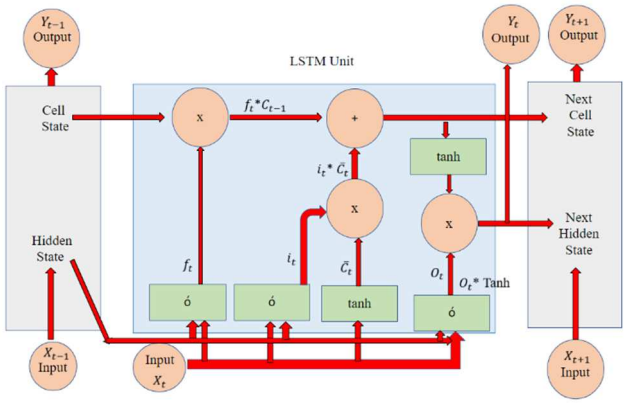


Fig. 4. Architecture of LSTM.

D. Evaluation Metrics

To evaluate and compare the efficiency of these supervised DL models, several evaluation metrics are used, namely Accuracy (*ACC*), Detection Rate (*DR*), Misdetection Rate (*MisR*), False Alarm Rate (*FAR*), Training Time Per Sample (*TTPS*), Prediction Time (*PT*), and Memory Size (*MR*). These metrics are defined as following:

- *ACC:* Total number of the correctly classified spoofed attacks and normal traffic over the whole number of the signals,
- *DR:* The rate of correctly classifying malicious signals as spoofed signals over the number of the spoofed signals.
- *MisR:* The rate of the spoofed signals that are classified wrongly as normal traffic over the number of the spoofed signals,
- *FAR:* The rate of normal traffic that are classified as spoofed signals over the number of the non-spoofed signals,
- *TTPS:* The time that is needed in the training process for every sample,

- *PT:* The time that is needed for classification, detection, and prediction of the samples in the given dataset,
- *MR:* The size of the memory during the training, testing, and validating of the DL model.

III. Results

In this study, to evaluate the performance of the selected models, we perform a 10-time re-sampling framework. Within every split, the corresponding data is partitioned into 60% training, 20% testing, and 20% validation. During the training process of DL models, using hyperparameters without any validation or even applying *K* cross-validation techniques may lead to over-fitting issues.

In addition, we investigate the values of the parameters used, which indicate exponential improvements in the models' performance. It is worth mentioning that Adaptive Moment Estimation (ADAM) optimizer and activation functions, namely Sigmoid and ReLu are used during the training, testing, and validating of the DL models. As we discussed, three supervised DL models, namely DNN, U-Net, and LSTM are used. Later, the classification models are trained, and the models are evaluated in terms of the selected metrics. These simulations are performed using intel core i7-10750H, 16.0 GB memory, and CPU of 2.60 GHz, for 200 Epochs and a batch size of 10. The results of these models are provided in Figure 6, and Tables II and III.

Fig. 5 and Table II represent the outcomes of our evaluation for supervised DL models in terms of the selected metrics. We observe that overall, the highest-performance model is obtained by U-Net, followed by DNN, and LSTM. It is noticed that the detection of GPS spoofing attacks using the U-Net model achieves a respectable testing accuracy of 98.80%, a probability of detection of 98.85%, a misdetection of 1.15%, a false alarm of 1.8%, a training time per sample of 0.22 seconds, a prediction time of 0.2 seconds, and a memory size of 199.87 MiB. In addition to this model, the DNN model provides satisfactory results and slightly lower performance than the U-Net model.

The DNN model achieves a testing accuracy of 94.3%, a probability of detection of 95.6%, a misdetection of 4.4%, a false alarm of 6.2%, a training time per sample of 0.40 seconds, a prediction time of 0.28 seconds, and a memory size of 235.19 MiB. In contrast, as shown in the following figure and table, the LSTM model has a lower testing accuracy of 92.9 % and a probability of detection of 93.1%, a higher misdetection of 6.9%, a false alarm of 8.2%, a training time per sample of 0.95 seconds, a prediction time of 0.25 seconds, and a memory size of 360.76 MiB. Similar observations can be found for training data on these DL models.

To summarize, from Figure 6, the accuracy and probability of detection of these selected supervised DL models reached at least 92% and above, while their probability of misdetection and false alarm are at most 8.2% and less. The best evaluation performance is obtained by the U-Net, although the LSTM is observed as the lowest performance model. Although the LSTM model is a powerful DL technique and performs well in time series data, it does not exceed the performance of the U-Net or DNN model. It is also worth mentioning that the training performance of these models is slightly better than their testing performance of them. In general, U-Net is a model that is spatially and temporally deep. Thus, according to our simulation results, the U-Net model has a high flexibility to be applied for detecting and classifying GPS attacks on UAVs.

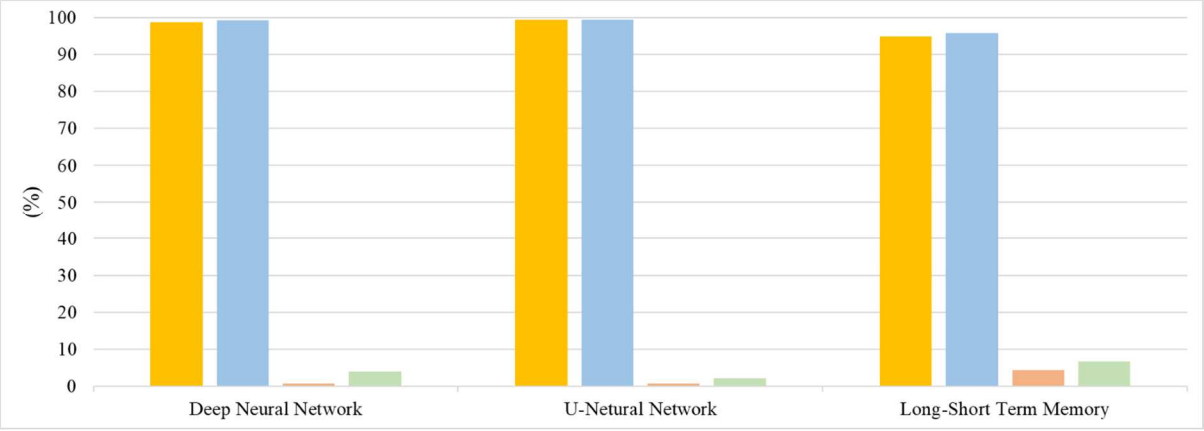
Table II. Training and Prediction Time and Memory Size Utilization per Sample for Supervised DL Models.

Model	Training Time Per Sample (Sec)	Prediction Time (Sec)	Memory Size (MiB)
DNN	0.40	0.18	235.19
U-Net	**0.22**	**0.2**	**199.87**
LSTM	0.95	0.25	360.76

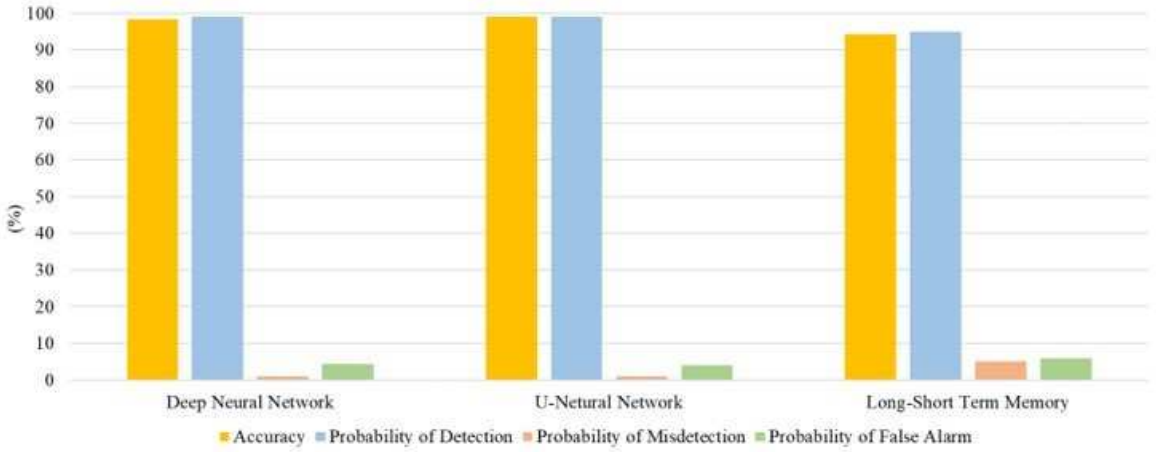
As it is clearly outlined in Table II, all timing and memory usage metrics of these supervised models are achieved good results, whereas the U-Net provides an excellent efficiency in terms of these metrics and can be considered an efficient DL model among other supervised models. Moreover, since U-Net consists of two parts, encoder and decoder, it can encode and extracts features and decode the results, resulting in a more efficient model, compared to other models.

In addition to these results, we provide a comprehensive comparison between our simulation results and other studies in literature. Table III provides a summary of our proposed models and current studies using DL models in detecting and classifying GPS spoofing attacks on UAVs. It is noticeable that most of the studies in literature only focused on supervised DL models; however, they discarded any investigation on detecting GPS Spoofing attacks on UAVs using unsupervised DL models. In addition, most of these studies used limited evaluation metrics, resulting in difficult interpretation of their results.

For instance, the authors of [13] proposed a DL model, namely an artificial neural network, to detect GPS spoofing attacks; however, they only used two metrics, namely True detection rate and detection time. According to their results, the proposed approach provided a high rate of true detection, although the detection time is significantly higher than the achieved results by the U-Net model. Also, in another study [12], the authors used an artificial neural network with high



A) Results on Training Data.



B) Results on Testing Data.

Fig. 5. Results of the Supervised Models on A) Training and B) Testing Data in terms of Accuracy, Probability of Detection, Misdetection, and False Alarm.

TABLE III. CURRENT STUDIES IN DETECTING GPS SPOOFING ATTACKS USING DL MODELS.

Ref.	Used Model(s)	Results
Proposed	**U-Net**	**Accuracy: 98.80%, Probability of detection: 98.85%, Probability of misdetection: 1.15%, Probability of false alarm: 1.8%, Training time per Sample: 0.22 Sec, Prediction time:0.2 Sec, Memory size: 199.87 MiB.**
[12]	Artificial Neural Network	Accuracy: 98.3%, Probability of detection: 99.2%, Probability of misdetection: 0.8%, Probability of false alarm of 2.6%.
[13]	Artificial Neural Network	True detection Probability: 99.35%, Detection time: 2.89 Sec.
[15]	Residual Neural Networks	Accuracy: 89.5%, Precision: 85.5%, Recall:95.4%, Error Rate: 0.105, F1-Score: 90.2%.

accuracy, detection rates, and low false alarm and misdetection rates. Despite these studies in the literature providing acceptable results, the lack of investigation into the efficiency of the proposed model makes it hard to compare these models with the other studies, including our study in the literature. It is also worth mentioning that this field of study is at an early stage, and the results in the literature still need to be improved.

Therefore, to address these challenges, this study fills the gap by comparing the performance of different supervised DL techniques from various categories, which outperform the existing works. To demonstrate the efficiency of the proposed models, we used timing and memory metrics. As a result, the U-Net provides satisfactory results, leading to a high potential to classify GPS spoofing attacks and normal traffic.

IV. Conclusion

Interest in detecting and classifying GPS spoofing attacks on UAVs has been exponentially increased in the last few years. For this purpose, several studies have been conducted to detect these vulnerabilities; however, this field of study still is at an early stage and needs to address the critical challenges, such as high misdetection and false alarm rates. This study aims to investigate the performance of different supervised and deep learning models in detecting GPS spoofing attacks on UAVs. The supervised deep learning models are classified into three types, namely artificial neural networks, convolutional neural networks, and recurrent neural networks. In these categories, three models of Deep Neural Network, U-Neural Network, and Long Short-term Memory are selected for training, testing, and validating the models. The evaluation was performed using seven metrics: accuracy, detection rate, misdetection rate, false alarm rate, training time per sample, prediction time, and memory size. The simulation results indicated that the U-Neural Network outperforms the other models in terms of these metrics.

Acknowledgments

The authors acknowledge the support of the National Science Foundation (NSF), Award Number 2006674.

References

[1] O. K. Isik, J. Hong, I. Petrunin, and A. Tsourdos, “Integrity Analysis for GPS-Based Navigation of UAVs in Urban Environment,” *Robotics*, vol. 9, no. 3, p. 66, 2020.

[2] G. Balamurugan, J. Valarmathi and V. P. S. Naidu, "Survey on UAV navigation in GPS denied environments," 2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES), pp. 198-204, 2016, doi: 10.1109/SCOPES.2016.7955787.

[3] J. Zhang, L. Pan, Q. -L. Han, C. Chen, S. Wen and Y. Xiang, "Deep Learning Based Attack Detection for Cyber-Physical System Cybersecurity: A Survey," in IEEE/CAA Journal of Automatica Sinica, vol. 9, no. 3, pp. 377-391, March 2022, doi: 10.1109/JAS.2021.1004261.

[4] T. Talaei Khoei, S. Ismail, K. A. Shamaileh, V. K. Devabhaktuni, and N. Kaabouch, “Impact of Dataset and Model Parameters on Machine Learning Performance for the Detection of GPS Spoofing Attacks on Unmanned Aerial Vehicles,” *Applied Sciences*, vol. 13, no. 1, p. 383, Dec. 2022, doi: 10.3390/app13010383.

[5] K. Kumar, S. Kumar, O. Kaiwartya, A. Sikandar, R. Kharel, and J. L. Mauri, “Internet of Unmanned Aerial Vehicles: QoS Provisioning in Aerial Ad-Hoc Networks,” *Sensors*, vol. 20, no. 11, p. 3160, 2020, doi: 10.3390/s20113160.

[6] K.-C. Kwon and D.-S. Shim, “Performance Analysis of Direct GPS Spoofing Detection Method with AHRS/Accelerometer,” *Sensors*, vol. 20, no. 4, p. 954, Feb. 2020, doi: 10.3390/s20040954.

[7] M. Varshosaz, A. Afary, B. Mojaradi, M. Saadatseresht, and E. Ghanbari Parmehr, “Spoofing Detection of Civilian UAVs Using Visual Odometry,” *ISPRS International Journal of Geo-Information*, vol. 9, no. 1, p. 6, Dec. 2019, doi: 10.3390/ijgi9010006.

[8] T. Talaei Khoei, S. Ismail, and N. Kaabouch, “Dynamic Selection Techniques for Detecting GPS Spoofing Attacks on UAVs,” *Sensors*, vol. 22, no. 2, p. 662, Jan. 2022, doi: 10.3390/s22020662.

[9] G. Aissou, H. O. Slimane, S. Benouadah and N. Kaabouch, "Tree-based Supervised Machine Learning Models For Detecting GPS Spoofing Attacks on UAS," 2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA, 2021, pp. 0649-0653, doi: 10.1109/UEMCON53757.2021.9666744.

[10] G. Aissou, S. Benouadah, H. El Alami and N. Kaabouch, "Instance-based Supervised Machine Learning Models for Detecting GPS Spoofing Attacks on UAS," 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 2022, pp. 0208-0214, doi: 10.1109/CCWC54503.2022.9720888.

[11] A. Shafique, A. Mehmood and M. Elhadef, "Detecting Signal Spoofing Attack in UAVs Using Machine Learning Models," in IEEE Access, vol. 9, pp. 93803-93815, 2021, doi: 10.1109/ACCESS.2021.3089847.

[12] M. R. Manesh, J. Kenney, W. C. Hu, V. K. Devabhaktuni, and N. Kaabouch, “Detection of GPS spoofing attacks on unmanned aerial systems,” in 2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC). IEEE, 2019, pp. 1–6.

[13] E. Shafiee, M. Mosavi, and M. Moazedi, “Detection of spoofing attack using machine learning based on multi-layer neural network in single frequency gps receivers,” The Journal of Navigation, vol. 71, no. 1, pp. 169–188, 2018.

[14] S. Wang, J. Wang, C. Su and X. Ma, "Intelligent Detection Algorithm Against UAVs' GPS Spoofing Attack," 2020 IEEE 26th International Conference on Parallel and Distributed Systems (ICPADS), Hong Kong, 2020, pp. 382-389, doi: 10.1109/ICPADS51040.2020.00058.

[15] N. Xue, N. Liang, H. Xianbin, L. Zhen, H. Larissa, and P. Christina, "Deepsim: Gps spoofing detection on uavs using satellite imagery matching." In Annual computer security applications conference, pp. 304-319. 2020.

[16] T. T. Khoei, A. Gasimova, M. A. Ahajjam, K. A. Shamaileh, V. Devabhaktuni and N. Kaabouch, "A Comparative Analysis of Supervised and Unsupervised Models for Detecting GPS Spoofing Attack on UAVs," 2022 IEEE International Conference on Electro Information Technology (eIT), Mankato, MN, USA, 2022, pp. 279-284, doi: 10.1109/eIT53891.2022.9813826.

[17] A. Gasimova, T. T. Khoei and N. Kaabouch, "A Comparative Analysis of the Ensemble Models for Detecting GPS Spoofing attacks on UAVs," 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 2022, pp. 0310-0315, doi: 10.1109/CCWC54503.2022.9720738.

[18] F. Jafari and S. Dorafshan, “Bridge Inspection and Defect Recognition with Using Impact Echo Data, Probability, and Naive Bayes Classifiers,” *Infrastructures*, vol. 6, no. 9, p. 132, 2021.

[19] T. Talaei Khoei and N. Kaabouch, “A Comparative Analysis of Supervised and Unsupervised Models for Detecting Attacks on the Intrusion Detection Systems,” *Information*, vol. 14, no. 2, p. 103, 2023.

[20] G. Montavon, W. Samek, and K. Müller, “Methods for interpreting and understanding deep neural networks. Digital signal processing,” 73, pp.1-15, 2018.

[21] O. Ronneberger, P. Fischer, and T. Brox, “U-net: Convolutional networks for biomedical image segmentation,” In International Conference on Medical image computing and computer-assisted intervention, pp. 234-241, Springer, Cham, 2015.

[22] A. Taylor, S. Leblanc, and N. Japkowicz,” Anomaly detection in automobile control network data with long short-term memory networks,” In 2016 IEEE International Conference on Data Science and Advanced Analytics (DSAA), pp. 130-139, 2016.