5G Radar and Wi-Fi based Machine Learning on Drone Detection and Localization

Mark Ignatius Teo
School of Computing Science
University of Glasgow
Glasgow, United Kingdom
2427225I@student.gla.ac.uk

Chee Kiat Seow
School of Computing Science
University of Glasgow
Glasgow, United Kingdom
CheeKiat.Seow@glasgow.ac.uk

Kai Wen
School of Electrical and Electronic Engineering
Nanyang Technological University
Singapore, Singapore
we0001ai@e.ntu.edu.sg

***Abstract*—Drone usages have been proliferating for various government initiatives, commercial benefits and civilian leisure purposes. Drone mismanagement especially civilian usage drones can easily expose threat and vulnerability of the Government Public Key Infrastructures (PKI) that hold crucial operations, affecting the survival and economic of the country. As such, detection and location identification of these drones are crucial immediately prior to their payload action. Existing drone detection solutions are bulky, expensive and hard to setup in real time. With the advent of 5G and Internet of Things (IoT), this paper proposes a cost effective bistatic radar solution that leverages on 5G cellular spectrum to detect the presence and localize the drone. Coupled with K-Nearest Neighbours (KNN) Machine Learning (ML) algorithm, the features of Non- Line of Sight (NLOS) transmissions by 5G radar and Received Signal Strength Indicator (RSSI) emitted by drone were used to predict the location of the drone. The proposed 5G radar solution can detect the presence of a drone in both outdoor and indoor environment with accuracy of 100%. Furthermore, it can localize the drone with an accuracy of up to 75%. These results have shown that a cost effective radar machine learning system, operating on the 5G cellular network spectrum can be developed to successfully identify and locate a drone in real-time.**

Keywords— Drone, 5G radar, line of sight, non-line of sight, machine learning

I. Introduction

Commercial Off-the-shelf (COTS) drones are widely available to consumers for leisure, business and entertainment activities. Unintentional, mischievous threat causes disrupted operations in Public Key Infrastructures (PKI) such as national event activities or airport operations while intentional threats such as malicious drones can compromise the confidentiality, integrity and availability (CIA) of these national locations/assets through espionage or property damage. There has been an increase in the number of cases where the drones are flown into such restricted air spaces which disrupt the operations within the vicinity [1]. Apart from errant users, COTS drones are also used in terrorism to drop malicious payloads or perform surveillance on restricted areas. This is very disturbing as what is commonly used in leisure and entertainment has been converted to a weapon of destruction. These attacks are quick and unsuspecting to the people in the vicinity catching everyone off guard [2]. With the advent of 5G cellular network which proliferate a lot of exciting applications using drone as the vehicle, drone navigation vulnerability using Global Positioning system (GPS) and 5G cellular has been proven to be spoofed by masquerade attackers [3].

The feasibility of detection and identification of drone has been demonstrated using neural network machine learning with COTS HackRF One Software Defined Radio (SDR) [4]. It was a passive detection in outdoor environment where the Wi-Fi Radio Frequency (RF) signals and its Service Set Identifier (SSID) were recorded before processing with neural network machine learning to classify the presence of a drone. There were many steps taken in identifying the presence of the drone where the drone could have flown off by the time the detection results came through. Furthermore, the solution is ineffective if the drone detection is performed in indoor environment where Wi-Fi signal strength from drone and other sources are similar. There are also other drone detection methods such as:

- RF Detection [4], [5] - Detecting the presence of a drone by capturing the RF emitted by the drone when communicating with the ground controller. In an open environment, it is possible to predict the location of a drone based on the difference in strength of the RF signals.
- Audio Based [6] - Detecting the presence of a drone using the sound emitted from the spinning propellers of the drone. This method is not very effective in a noise polluted environment.
- Locality Based [7]–[10] - Using localization techniques to identify the location of a drone.
- Radar Based [11]–[14] - Different configurations of bistatic radars to identify and locate the drone which is costly and impractical unless for military purposes.

There exists a need for cost effective active drone detection methods for either commercial or governmental purposes. In this paper, it explores the possibility of drone detection and its location identification using a bistatic radar [15] which operates on the 5G network cellular spectrum. The bistatic radar detects the presence of a drone by capturing the 5G Non-Line of Sight (NLOS) transmissions reflected off the body of the drone, and the Wi-Fi Received Signal Strength Indicator (RSSI) emission of the drone captured by a RF spectrum ground controller. Furthermore, we proposed a novel K-Nearest Neighbour (KNN) Machine Learning (ML) that leverages on these two signatures to perform real-time location prediction of the drone based on the instantaneous signature data captured. This paper aims to create a easily deployable 5G radar system that is effective yet efficient in alerting the users of the presence and location of the drone. The proposed solution helps to minimize the CIA damages and intrusions by these drones on the property through early detection, in both the indoor and outdoor environments. Experimental campaign have shown that 100% detection accuracy achieved in both indoor and outdoor environment with localization accuracy of up to 75%. Furthermore, the proposed radar system can also be adapted to leverage on the local 5G network infrastructure to perform detection, which will further reduce the CAPEX and OPEX cost to setup and maintain the radar ML system. Section II outlines the design and implementation while Section III explains on the KNN machine learning algorithm processes. Section IV describes the experimental campaign and evaluation followed by conclusion in section V.

II. SYSTEM DESIGN AND IMPLEMENTATION

The deployment of the 5G radar and RSSI receiver system is shown in Figure 1. This setup operates on 3 HackRF One SDRs. Two of the HackRF SDRs serves as 5G signal transmitter (Tx) and receiver (Rx) while the other HackRF SDR as Wi-Fi RSSI receiver to perform spectrum scanning to capture the Wi-Fi RSSI emission from the drone as depicts in Figure 2. These three SDRs work together to collect the Line of Sight (LOS), NLOS signal transmissions by the 5G radar system and RSSI signal emission by the drone within the square grid. These signature data will then be processed in the KNN ML for prediction. The Tx and Rx are implemented using GNU Radio Companion (GRC) that enables users to program operations on the HackRF One SDR. The Tx and Rx focus on capturing the 5G LOS/NLOS transmissions while the RSSI receiver uses the HackRF Sweep Spectrum Analyser (HSSA) to capture RSSI values of the drone and the environment. The range of the radar can be expanded by simply adding more HackRF One SDRs to create more grid boxes for detection and localization of the drone.

The setup was deployed in both outdoor and indoor environment which is shown in Figure 3 to test the effectiveness in receiving the 5G LOS, NLOS transmissions, RSSI values of the flying drones and hence robustness of KNN ML prediction. In the indoor urban environment especially enclosed Wi-Fi crowded environment, it is expected to have more multi-path effects as there are more objects present that would result in multiple NLOS specular, non-specular reflection, diffraction and interference.

A. 5G Transmitter

To achieve consistent transmissions between the Tx and Rx at the distance of $2\sqrt{2}$ m, the following equations were used to calculate the Free-Space Path Loss (FSPL). It is important to understand how the FSPL is affected by distance between the transmitter and receiver which can cause the strength of a transmitted signal to drop. This could affect how well the Rx receives the signals over different distances. The first equation determines how the electromagnetic energy is spread in free space. This equation is called the inverse square law and is as such,

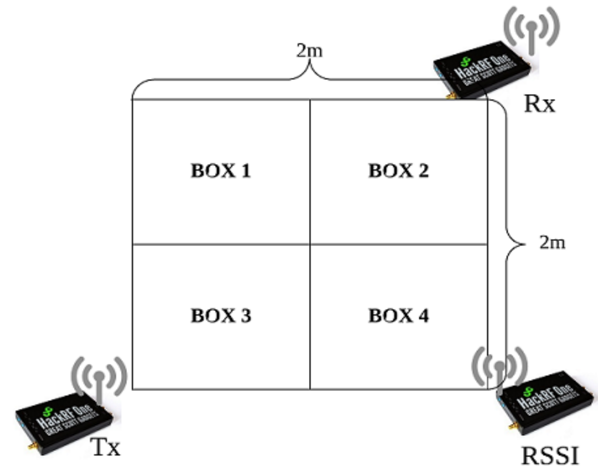

Fig. 1. Deployment of Radar

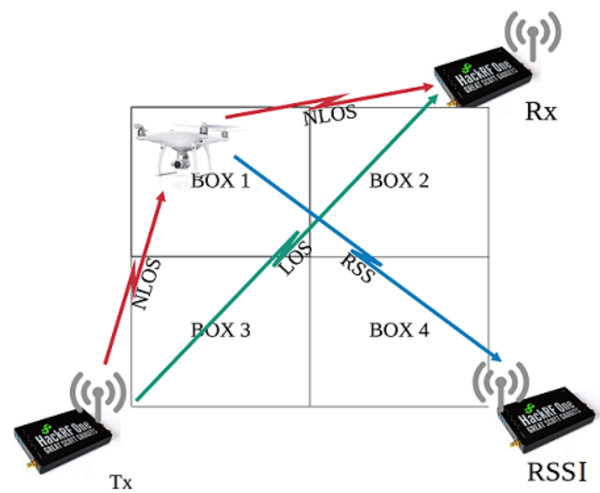

Fig. 2. NLOS Detection

$$S=\frac{P_t}{4\pi R^2} \quad (1)$$

where S is the power per unit area at distance, P_t is the transmitted power in Watts (W) and R is the distance in metres (m) between the transmitter and receiver.

Fig. 3. Outdoor (left) and Indoor (right) Environment

The second equation determines how well the Rx can receive the transmitted signal by the Tx. The equation is defined as such,

$$P_r = \frac{S_r \cdot \lambda^2}{4\pi} \quad (2)$$

where P_r is the received power (W), S_r is the non-directional received power density and λ is the transmitted wavelength (m).

Lastly, the total FSPL loss can be determined by the following ratio,

$$\text{FSPL} = \frac{P_t}{P_r} = \left(\frac{4\pi R}{\lambda}\right)^2 = \left(\frac{4\pi Rf}{c}\right)^2 \quad (3)$$

where f is the transmitted frequency and c is the speed of light. By knowing the FSPL, the transmitting strength of the Tx antenna can be calculated and configured accordingly in GRC.

The Tx transmits a file every six seconds via the HackRF One on the 5G frequency of 2.6 GHz. Before the file is transmitted, the contents of the file are set. The epoch timestamp of the transmission is appended to the back of the blank file. By appending the timestamp to the contents of the file, it acts as a marker for the receiver to know the current interval. Once the transmission is complete, the file is reverted back to its clean state so that the next timestamp can be appended to the file without increasing the file size as the program runs for more iterations.

B. 5G Receiver

The receiving phase listens for the packets that the Tx HackRF One broadcasts on the frequency of 2.6 GHz. Once the packets are received, the contents of the packets are logged. Whilst the log file continues to receive data, a python script analyzes the contents of the log file. This analysis is performed in real-time and can detect transmission errors. It detects new timestamps and timestamps that have arrived late or in the wrong order. New timestamps indicate that the transmitter has moved on to the next interval of transmissions and it is classified as a LOS transmission. Whereas for incomplete timestamps, they indicate a disruption to the flow of transmission between the Tx and Rx which is classified as a NLOS transmission.

C. RSSI Receiver

The Wi-Fi RSSI receiver utilizes the command "hackrf_sweep -f 2400:2490 -r fileoutput.csv" to listen and record the RSSI in the environment. The arguments for the commands are as follows:

- hackrf_sweep is a command to perform sweeping of the specified frequency spectrum.
- -f specifies the frequency range to scan on in MHz. The frequency of 2400MHz to 2490MHz was chosen as the DJI drone used in this paper operates within that frequency range.
- -r specifies the file to output the data to. For this paper, the data was collected in a Comma Separated Value (CSV) file.

By retrieving the RSSI, the data signature of RSSI for each location can be acquired. When there is no presence of a drone, the environment noise level can be observed to be on the average of -70 dBm across the frequency range of 2.4GHz to 2.49GHz. However, when drone is present, there is a prominent spike in the received spectrum, and it is often located in the operating frequency range of the DJI drone. The drastic spike in RSSI values when the drone is present makes it viable for use as a feature signature. It can also be observed that when the drone is closer to the RSSI Receiver, the RSSI tends to be stronger and when it is further, the signal may be weaker but still stronger than the baseline environment noise, obeying the FSPL calculation.

III. Machine Learning Process

The ML algorithm used in this paper is KNN algorithm that requires minimal training and can make quick real time predictions as compared to NN used in [4]. By identifying patterns and calculating the Euclidean Distance (ED) between clusters of training data points and test data points, KNN is able to classify the test data point to the closest cluster and provide a label for it. To calculate the distance between two groups of values, the equation below is used,

$$\text{dist}(\mathbf{a},\mathbf{b})_k = w_k \sqrt{\sum_{i=1}^{n} \sum_{j=1}^{m} \left(a_{i,k} - b_{j,k}\right)^2} \quad (4)$$

where n and m are the number of training and test data points while $a_{i,k}$ and $b_{j,k}$ represent the feature k of training point i and test point j respectively. The features can be combined using weight w_k if they are comparable where $\sum w_k = 1$.

There are four processes which the data undergoes before it is used for training or testing. This process is very important to enable the ML model to understand the data and identify the features to it so that it can be used to make prediction.

A. Data Collection

In this phase, the time of arrival (TOA) for 5G LOS/NLOS transmission, and the RSSI of the environment and the drone, were collected. To create a unique signature in each box, the data collection was run separately for each box. To identify the "No Drone" scenario, the data collection occurred when there was no drone flown within the grid. The deployment of the data collection is depicted in Figures 1 and 2. The data collection was performed in both indoor and outdoor environment to facilitate collection of more diverse environment channel patterns since the advent of 5G and IoT accelerate applications that leverage on usage of drone in both open and indoor urban environments. During the data collection, both 50 data points of 5G LOS transmission for the "No Drone" scenario and 50 data points of 5G NLOS transmissions for the "Drone" scenario on each grid box were collected. The RSSI values measured at the RSSI receiver were also collected during the absence and presence of drone.

B. Data Pre-Processing

In this phase, the collected 5G LOS/NLOS transmissions data are matched with the respective highest RSSI value received at the point of transmission. This enables the ML model to know how a 5G LOS/NLOS transmission relates to the respective RSSI value. That is to say that the stronger RSSI values usually mean that there is an 5G NLOS transmission due to the drone being present, whereas for the 5G LOS transmission (no drone), the RSSI value is closer to the environmental RSSI level. The data is also labelled to identify the classification that the data point belongs to. This classification will be used to train the ML model to classify the data points and verify the test results.

C. *Feature Extraction*

In this phase, the features are placed into histograms in Figures 4 and 5 to discover the trend in the data and identify ways that the data can be fitted into the ML model for training as well as testing. There are five classes that a data can be classified to, "No Drone", "Box 1", "Box 2", "Box 3" and "Box4".

In normal cases of KNN, depending on the *n* value, the test data point is compared against *n* number of training data points that are closest to it. The label with the highest count amongst the training data point is selected. However, for this application, since the individual RSSI values and 5G LOS/NLOS transmission times are not distinct enough to identify a box within the grid, the training points are grouped together to form a cluster of training points. As such when drone is present in each box in the grid and for the "No Drone" scenario, the training cluster has a group of 40 data points respectively. Thus in this paper, the *n* value is set as 40. This enables the ML model to better identify the patterns over each box in the grid based on the 5G LOS/NLOS transmission times and RSSI values. After identifying the patterns in different environments in terms of 5G LOS/NLOS timings and the RSSI values as shown in Figure 4 and 5, the following are the objectives that ML model will be trained to perform:

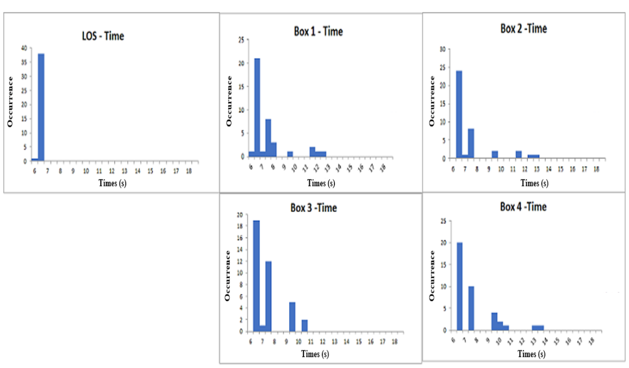

Fig. 4. Histogram of the Outdoor 5G LOS/NLOS Transmission Timings

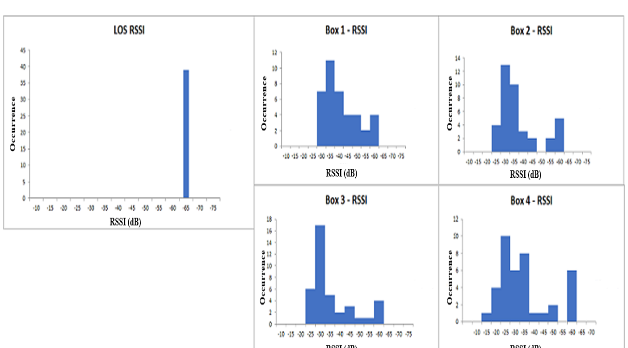

Fig. 5. Histogram of Outdoor RSSI Values

- Identifying if a drone is present, based on 5G LOS/NLOS transmissions.
- Identifying which Box is the drone in, based on 5G NLOS transmissions.
- Identifying which Box is the drone in, based on 5G RSSI values.

D. *Training ML Model*

Once the features have been extracted, it can be used to train the ML model. The ML model will be trained to identify the ED between the trained data points and the test data point. The label with the minimal ED from the test data point will be awarded as the classification of that data point. The model will be trained to perform the classification in two phases as shown in Figure 6. By breaking down the classification process into two phases, the ML's performance can be evaluated individually in the different phases.

In reference to Figure 6, there are two processes namely detection and localization phases as shown by highlighted green box and orange box respectively. In the detection phase, the input data is the 5G LOS/NLOS transmission timings and the RSSI values which will be used to evaluate distinguish between a 5G LOS or NLOS transmission. If it is a LOS transmission, it indicates the absence of drone else it is deemed as a NLOS transmission. The ML will proceed in the localization phase to classify among the 4 boxes using the NLOS and the RSSI training data disjointedly to determine the box with the lowest ED from the test data point. We will choose the box localization solution that has the lowest ED as the estimated location of the identified drone.

We will evaluate how the features affect the performance of either using 5G NLOS transmission or RSSI box classification individually. When testing the ML's performance, the test data points are clustered similar to the training data points where one test data cluster consists of 10 data points with the same classification.

E. *Evaluating ML Model*

To evaluate the ML model, confusion matrix was used. This allowed the ML's accuracy, precision, recall and F1-score to be obtained. Since there are multiple ways to classify the predictions, the flow of the ML was broken down. By breaking down the predictions to different stages, the ML's performance can be better evaluated. In this paper, the True Positive (TP),

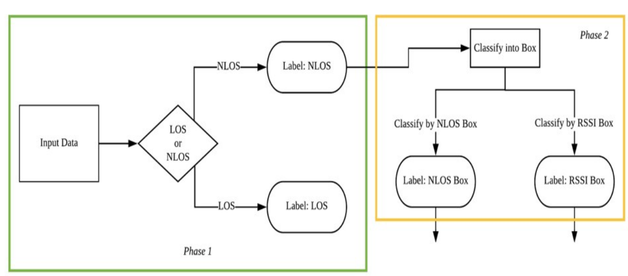

Fig. 6. ML Classification Process

False Positive (FP), True Negative (TN) and False Negative (FN) are defined as such:

- TP - When a drone is present, the prediction accurately returns that a drone is present.
- FP - When a drone is not present, the prediction says that the drone is present.
- TN - When a drone is not present, the prediction accurately returns that a drone is not present.
- FN - When a drone is present, the prediction says that the drone is not present.

By using the confusion matrix, the Accuracy, Precision and Recall of the ML model can be evaluated at each stage of the classification process. There are several scenarios that can be expected when evaluating the performance of the classifications.

- High FNs - When there are more FNs predicted that is not acceptable because it indicates that the ML cannot detect the presence of a drone. This can be a danger to the users as the drone will be present without them knowing.
- High FPs - When there are more FPs, it means that the drone's presence is detected but the location cannot be deduced. This is still acceptable as the ML is able to detect the presence of a drone.
- High TPs and TNs - Large number of TP and TN indicates that the ML is able to perform predictions with a very high accuracy. This indicates that the ML is well trained.

IV. Evaluation

A. *Detection of Drone Presence using LOS and NLOS*

The ML successfully classified between 5G LOS/NLOS transmissions successfully, achieving 100% accuracy indicating the absence and presence of drone as shown in Table 1. This shows that the 5G radar employed with ML can detect a drone's presence as LOS/NLOS features are very distinct from one another. This demonstrates the feasibility of detection of those stealth drones that have its own controlled RF channel which is operating at non Wi-Fi band.

TABLE I. PERFORMANCE METRICS FOR LOS/NLOS CLASSIFICATION (INDOOR & OUTDOOR)

LOS & NLOS Classification				
Label	**Precision**	**Recall**	**f1-score**	**Support**
LOS	1.00	1.00	1.00	2
NLOS	1.00	1.00	1.00	8

B. *Identifying Drone Location with NLOS Transmissions*

The ML has an accuracy of 25% in predicting the location of the drone using 5G NLOS transmissions. This is due to the similarities in 5G NLOS transmission values across all boxes. This makes it hard for the ML to differentiate between boxes and the ED will be closest to the box with the best spread of data points. Therefore, relying on 5G NLOS transmissions alone as a feature for the ML is not the best option. It also provide an indicator that the ML performance will improve if area of coverage is larger since propagation path delay will be longer, which leads to more distinct 5G NLOS timings in different coverage region.

TABLE II. PERFORMANCE MATRIX FOR NLOS BOX CLASSIFICATION

	Indoor			
Label	**Precision**	**Recall**	**f1-score**	**Support**
1	0.00	0.00	0.00	1
2	0.00	0.00	0.00	1
3	0.00	0.00	0.00	1
4	0.25	1.00	0.40	1
	Outdoor			
Label	**Precision**	**Recall**	**f1-score**	**Support**
1	0.00	0.00	0.00	1
2	0.00	0.00	0.00	1
3	0.00	0.00	0.00	1
4	0.25	1.00	0.40	1

C. *Identifying Drone Location with RSSI Values*

The ML is able to achieve 75% accuracy in identifying the location of the drone in the boxes for the indoor setting but with an accuracy of 25% for the outdoor setting. The RSSI values for the outdoor may be similar since the strength of RSSI depends on the location of the RSSI receiver, thus in an outdoor space, the freedom of height makes it viable for a box that is closer to the receiver to receive a weaker RSSI value when the drone is at a higher height. Whereas in the indoor environment, the drone has limited heights, therefore the drone's RSSI strength is more consistent and distinct as the drone will have to fly within the limited space thus being closer to the receiver.

However, in the indoor context, there are multi-path effects as well that could create confusion between boxes such as Box 3 and 4 in Table III.

TABLE III. PERFORMANCE METRICS FOR RSSI BOX CLASSIFICATION

	Indoor			
Label	**Precision**	**Recall**	**f1-score**	**Support**
1	1.00	1.00	1.00	1
2	1.00	1.00	1.00	1
3	0.00	0.00	0.00	1
4	0.50	1.00	0.67	1
	Outdoor			
Label	**Precision**	**Recall**	**f1-score**	**Support**
1	0.00	0.00	0.00	1
2	0.00	0.00	0.00	1
3	0.00	0.00	0.00	1
4	0.33	1.00	0.50	1

D. *Overall ML Performance*

The overall performance in both environments differs substantially in both indoor and outdoor environment. In the outdoor environment, the predictions were consistent across both 5G NLOS and RSSI data with 25% accuracy. Whereas for the indoor environment, the RSSI tends to perform better than the 5G NLOS radar as indoor environment has richer feature representation in RSSI data than outdoor environment due to the abundance of clutters achieving 75% accuracy.

Since predictions can be made in both environments, the ML model is suitable to be deployed. It is noteworthy that the KNN ML did not make any FN predictions which is very important to ensure no drone is go undetected and non localized. The high FP results can be countered with more data collection in different environments so that the ML model can have more groups of data points to train with and test against. Therefore, the 5G radar is suitable to be deployed with ML in both environments.

V. Conclusion

This project proposes a novel cost-effective drone detection method using a bistatic radar operating on the 5G mid-band spectrum. This radar detects the presence of a drone through the disruption of 5G LOS transmissions. These disruptions are known as 5G NLOS transmissions reflected off the body of a drone. The system also captures the RSSI values of the environment which are used to identify the drone signal strengths at different locations. The bistatic radar system has shown to provide a way to locate the drone within a 2x2 grid of 1m in length. To bring in an additional novelty, a supervised ML algorithm, KNN, was adopted to perform predictions whether a drone is present and where the drone may be located in the grid using the 5G NLOS and RSSI features. Experiments were conducted in both indoor and outdoor environments, and the ML's performance was evaluated. In both environments, the ML model successfully identified the presence of a drone using 5G LOS/NLOS transmissions achieving an accuracy of 100%. The predictions based on the individual features of 5G NLOS transmissions and RSSI values, has an accuracy of 25% and 25%-75% respectively. Despite the fluctuations in accuracy, the ML has achieved a zero FN results which is important as it shows that it can detect the presence of a drone.

This proposed system is both novel and cost-effective. It has proved that a cost-effective system like this, can perform real time detection of the drones with zero FN results. This system can be deployed in the indoors and outdoors to detect and identify the location of a drone. In future, the size of environments can be expanded to further test the proposed method while multiple drones identification and localization is another noteworthy research area to look into.

References

[1] Channel News Asia, "Drone sightings at Changi Airport force closure of one runway, nearly 40 flights affected", 2019-06-19, https://www.channelnewsasia.com/news/singapore/changi-airport-drone- sightings-one-runway-closed-11641920, Accessed: 2020-01-11.

[2] Yaacoub, J. P., Noura, H., Salman, O., Chehab, A. (2020). "Security analysis of drones systems: Attacks, limitations, and recommendations." Internet of Things, 11, 100218.

[3] R.Y. Zhang, C.K. Seow, K. Wen and H. Zhang, "Spoofing attack of Drone", 2018 IEEE 4th International Conference on Computer and Communications (ICCC), Chengdu, China, Dec 2018, pp.1239-1246.

[4] Y.J.J.Teoh and C.K.Seow,"RF and Network Signature-based Machine Learning on Detection of Wireless Controlled Drone," 2019 PhotonIcs & Electromagnetics Research Symposium - Spring (PIERS-Spring), Rome, Italy, June 2019, pp. 408-417.

[5] Phuc Nguyen, Mahesh Ravindranatha, Anh Nguyen, Richard Han, and Tam Vu, 2016. "Investigating Cost-effective RF-based Detection of Drones." In Proceedings of the 2nd Workshop on Micro Aerial Vehicle Networks, Systems, and Applications for Civilian Use (DroNet '16). Association for Computing Machinery, New York, NY, USA, 17–22.

[6] N.Siriphun, S.Kashihara, D.Fall, and A.Khurat,"DistinguishingDrone Types Based on Acoustic Wave by IoT Device," 2018 22nd International Computer Science and Engineering Conference (ICSEC), Chiang Mai, Thailand, 2018, pp. 1-4.

[7] H. Zhang, S.Y. Tan, and C.K. Seow , "TOA-Based Indoor localization and tracking with inaccurate floor plan map via MRMSC-PHD Filter ", IEEE Sensors Journal , vol. 19, Issue 21, pp 9869-9882, Nov. 2019.

[8] Chen, S., S. Y. Tan, and C. K. Seow, "Peer-to-peer localization in urban and indoor environments," Progress In Electromagnetics Research B, Vol. 33, 339–358, 2011.

[9] K. Wen, C. K. Seow, and S. Y. Tan, "An Indoor Localization and Tracking System Using Succesive Weighted RSS Projection," IEEE Antennas and Wireless Propagation Letters , vol. 19, Issue 9, pp 1620-1624, Sept. 2020.

[10] C. K. Seow and S. Y. Tan, "Non-line-of-sight unidirectional mobile localisation in multipath environment," in Electronics Letters, vol. 44, no. 2, pp. 141-142, 17 January 2008.

[11] B. Nuss, L. Sit, M. Fennel, J. Mayer, T. Mahler, and T. Zwick, "MIMO OFDM radar system for drone detection," 2017 18th International Radar Symposium (IRS), Prague, 2017, pp. 1-9.

[12] D. Solomitckii, M. Gapeyenko, V. Semkin, S. Andreev, and Y. Koucheryavy, "Technologies for Efficient Amateur Drone Detection in 5G Millimeter-Wave Cellular Infrastructure," in IEEE Communications Magazine, vol. 56, no. 1, pp. 43-50, Jan. 2018.

[13] G. Sacco, E. Pittella, S. Pisa, and E. Piuzzi, "A MISO Radar System for Drone Localization," 2018 5th IEEE International Workshop on Metrology for AeroSpace (MetroAeroSpace), Rome, 2018, pp. 549-553.

[14] G. Gaigals and E. Vavilina, "Simulation of compressed sensing based passive radar for drone detection," 2017 5th IEEE Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE), Riga, 2017, pp. 1-5.

[15] R. J. Burkholder, L. J. Gupta, and J. T. Johnson, "Comparison of monostatic and bistatic radar images," in IEEE Antennas and Propagation Magazine, vol. 45, no. 3, pp. 41-50, June 2003.