# Threat Detection in Hostile Environment with Deep Learning based on Drone's Vision

**Sufiyan Shaikh[1], Rushikesh Raskar[2], Lajri Pande[3], Zeenat Khan[4], Prof Shweta P.Guja[5]**

*[1,2,3,4] B.E student, Dept. of computer, NBN Sinhgad School of Engineering, Ambegaon, Pune-411041, Maharashtra, India*

*[5] Prof. ,Dept of Engineering, NBN Sinhgad School of Engineering, Ambegaon, Pune-411041, Maharashtra, India*

***Abstract***

*We have consider a video surveillance system, using a camera which is mount on a drone flying over the area that has to be monitored and send the video to a control center. The resulting network that we have to get composed of a static components, and a moving components on (Drone). The video signal will be transferred via radio signal to the control center. The control center will be equipped with AI/Ml enabled application which will be able to detect what is in the frame. This system is very useful in hostile environment where we need to examine the whole area before proceeding and where the involvement of human being is dangerous to his life. This drone will the video feed with minimum to very low latency. The drone will be stealth and will make low noise which will make it difficult to be easily noticed.*

***Keywords**: Artificial Intelligence (AI) and Machine Learning (ML).*

## I. INTRODUCTION

Nowadays, the demand and interest in drones are increased very much. Due to this increase in demands, drone merchandise of newer types are being manufactured and designed, so people buy them at affords price for many purposes (i.e., research purpose, Aerial , Agriculture & Farming , etc.). In day to day life drone industry keep grows in increasing order.

There has been a massive production in commercial drones to satisfy the civilian's needs, but this has a drawback. As it has now become we can easily to spot drones in outfield, more safety relating issue we brought up as concern. Those drones are not merely about accidents relating to drone harm individuals, but also drone include which invade government restricted area. Consider drone is fast in surrounding area and he can do all those things, people can't recognize drone is bigger threat than people would imagine. As a number of drones out in publically areas are increasing, it has become harder to regulate them safely and legally. When it comes on detection are we will do the first thing that comes in our mind is radars. Radar can be bigger or smaller in size depending upon the application.

We propose a things drone detection system based on machine learning, artificial intelligence as an alternative option for above mentioned matters. The system will capture the object detection to any possible threats in the image in one format, so we can recognize easily. Our system can also be applies on an environment with surveillance drones with the following scenario. In a mission, the surveillance drone will take off from the start position and fly to a specified point and then record its surroundings on camera. If there is any vulnerability or threats in that area, it's captured the video from frame by applying object detection algorithm and the system will be mark the frame. The marked frame and detected objects will then be used further module. The system can be learned about various threats through machine learning will identify the threat by using the model. Such-system can be applied to another surveillance system as a complement it can be applied to the others to find unknown threats (drones), detect it, and show some output, by defining the name.

For image processing, the system uses GPU with CUDA programming on the video frames we have used. In each of the frame, the object detection algorithm used will be applies to the environment of the threat in the video frames. Specify, the YOLO algorithm is used for object detection in any format. With the helping of the machine learning algorithm based on various threaten images, which are given and processed beforehand on the system, the system will learns how to detect the threats accurately from frames, and show some featured output. The frames with threats detects are processing again to identify the threat model.

## II. RELATED WORK

In this part, would like to talk about various researches that are similar to our research. The goal or main motive of our paper can be summarized as detection and identification of threats using drone on image processing, machine learning and artificial intelligence.

We have applied YOLO algorithm for threat detection. The techniques have three key characteristics. First, using Integral Image, features the detectors are using can be compute quickly, which makes its computational capacity O (1). Second, the classifier by select a small number feature which are important using a learning algorithm yields a efficient classifier[5 6]. Third, the method of combining more complex classifiers which will cascaded fashion makes it will be very fast.

Recently, deep learning is used in many studies of image processing field. Among the deep neural network structures, Convolution Neural Network (CNN) is gain the information interest because it automatically detects the features which are important in its learns and knowing phase and easily analyze. It has shows performance breakthroughs in image classification, object detection and object classification. The reason due to which CNN shows high performances in extracted feature is its capability of extracting abstract features. This allows it to process with great accuracy and more accurate information.

The threat identification and detection is done using supervised learning. Supervised learning is systematically more adjusted CNN, and have been applied. It has gains the information to the recognition by showing better performances than that of unsupervised learning. Based on the researches, we choose CNN to increasing speed and efficiency of that system. The two modules implement in our system require learning based on images and identify the object. As our system is heavily relies on machine learning, with careful calibration and sufficient learning module, the system can show far better performance.

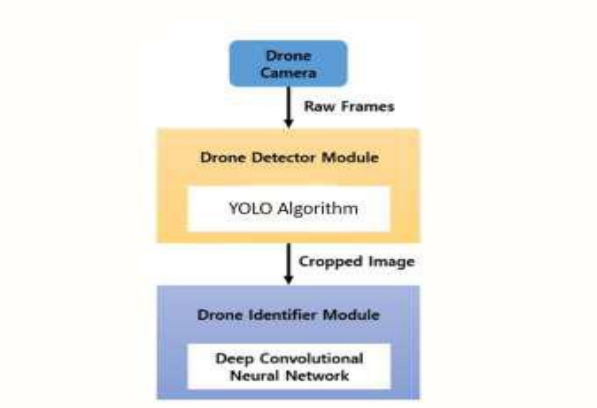


Figure. 1: Drone Identification and Detection System.

## III. SYSTEM IMPLEMENTATION AND DESIGN

In this part, we describe the system propose by us and implementation details of the same. We will first explain the overall system and then describe the overall modules.

### A. **Overall System**

The above proposed system is designed such that it will top computing board established on each surveillance drones and gives use information.

**Batteries :** In Order to differentiate our Drone from other drones we tried to increase the flight time by using two batteries in parallel one is 5400mAh and other is 3300mAh 3s Lithium Polymer Batteries. LiPo, also referred Lithium Polymer batteries are newer kind of battery used in electronic device. These batteries are gaining immense Popularity over the past few years because of their log run times and high power.

After all those things and process we described in the above Fig.1, the drones are to be reported to the Ground Control Station.

### B. **Threat Detector Module**

The threat detector is a module which detects threats on video frames that is taken by the camera on the drones which is transmission form sender to receiver information. Accurate 2D detection of the threat on the frames is most important to the overall system. Therefore, in order to ensure that accuracy while also maintaining speed, our system uses YOLO algorithm and Open Computer Vision library. For training of the classifier module, we have used 2089 positive example and 3018 negative example. We have collected the positive examples from Google, and manually cropped the drone from every image and give information about it. Negative examples were collects from http://face.urtho.net/. After applies image distortion on the positive example, we expanded our positive examples to 7001. Based on these positive image, we have train our Classifier. Our System uses Analogue video Signal for detection purpose. The trained classifier will find the 2D or 3D area on the frames, where the threat has been located then area will cropped, and passed on to the drone identifier module then he will classify it and give info about it.

### C. **Threat Identifier Module**

The threat identification module that will classify the unknowns threats to send a vendors model on the basis of the crop image. To identify which type of threats, a CNN will be constructs. Threat identification and threat detection can also be done by other types of deep learning methods such as ResNet or Raster R-CNN. However the depth of the image, it would be taking a very long time for training, and the complexity will goes to high. In order to overcome this, we have separated the system into a classifier and accordingly CNN will be processing. Additionally, this will also allow us to train faster with only fewer images. The CNN consists of two layer and two connected layers. Each of the fully connect layers will be implemented with a 30 percent dropouts. The Activation functions, Rectifies the Linear Unit (ReLu) is used, and Adaptive Motion Estimation (Adam) is used for the gradient descent algorithm for making the system and helps the identify the module easily.

## IV. PERFOMANCE EVALUAITON

In above part, we will show our experimentation result and performance analysis and we have decided. First, we show how the threat detection module will work and how will be analyzed the performance of the threat identifier module. In the system, we use the YOLO for detection of objects. YOLO is a very fast real-time algorithm used for multi-object detection in our system. YOLO means “You Only Look Once”. These algorithms will apply neural networks to the entire images. The image will be divided by the network into S x S grid and will give the result with bounded boxes, which are nothing but boxes drawn at the background of the images and predict the probability of that region. Logistic regression is a method come up with these probability. The bounded boxes will be weighted by the associate probabilities. For class predictions and independent logistic classifier will be use.

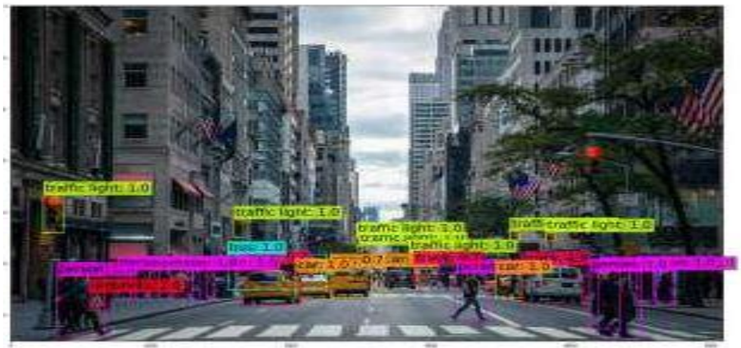


Figure 2. Object Detect using YOLO algorithm

### A. **Threat Detector Experiment**

The detector module has learn some phases, before running the threat detector module. It is required to learning phase, the images collected from Google will be used supervised learning module used for the drone detectors. After these following positive example images, we will prepare these test images near about 829 in order of the test the performance of the system. The test images will not used for learning phase, and are only used for evaluation of the performance. This is done in order to validates the system can detect threats from another images that it is not been exposed to earlier module. The detection will give the result on that threat detector module. As shown in the image, if we find image, then it will find particular area, then there is an expected threat , will marked by using a rectangular box.

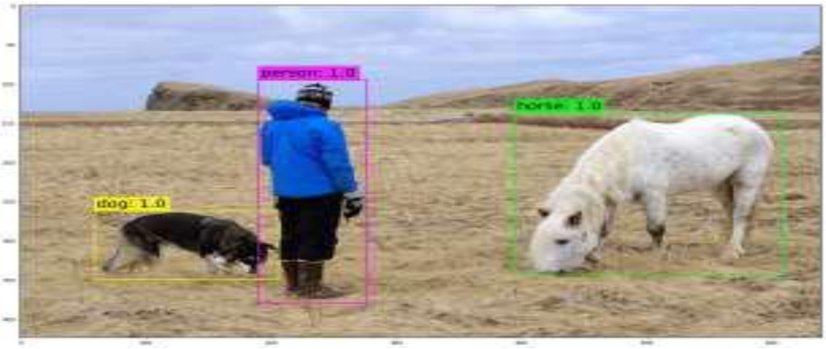
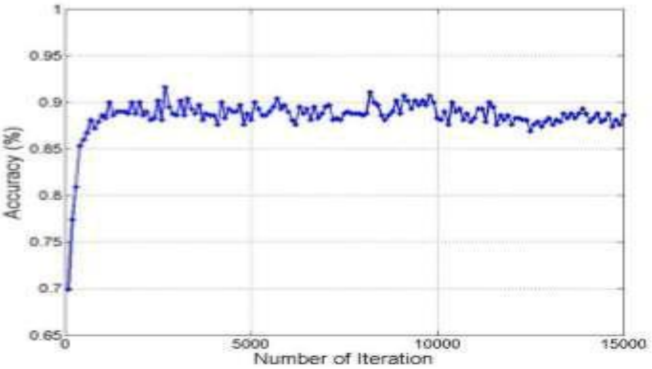


Figure. 3 Threat Identifier

The threat identifier module is used to identifies the threat using above system. The 2088 positive image examples will all be manually labeled. The positive example images which are around 1777 image were used for training, and the remaining above examples we are used for evaluation of the test image. A Mini-batch with 256 batch size is used for training phase. The threat identification module shows maximum accuracy of that given image in percentage format. False classification is only made in cases which are challenges for the human eyes too. In below fig the system will reaches the maximum accuracy with a few iteration, and saturated around above given some percent format.

This experiment proved that deep neural network CNN is used for classifies the threat by model using a drone with a camera. Additional information, it also shows that it doesn’t require much training data for training purpose.



## V. CONCLUSIONS

In our paper, we proposes a threats detection module and identification system which make decisions on the basis of video obtain from a drone camera which is place on a drone. In our system proves that even using simple artificial intelligence technique used, the performances are efficient. All systems are actual implements, and train the data was collected from the internet sources. Uses small amount of easily collected data, the system will shows great accuracy, which will makes it even more appealing. For future purpose, we would definitely like to develop system and distance estimation module which will complements our existing system module. Based on the image, estimating the distance between the drone and the unknown threats can be valuable information which will be used for tracking the module and we calculate the distance from the threat and drone. Along with private drones are being massively produced to satisfy the civilian's needs and help with those people, there have been some downsides to this as well.

As it has become easier to environment to identify drone in outdoor, more safety issue are being brought up as concern. These are not even knows about accident regards drone harming individuals, but also those drones are invading government restricted area.

The major need for this type of technology will be in the area of detection. The drone can be used for detecting harmful threads; it can be used for detecting any vulnerability in the crowded areas. The system which will internally can be trained to detect anything with maximum possible accuracy.

The camera mounted on the drone will feed the video signal to the algorithm which will identify the elements of interest and create a bounding box and also predict the probability of accuracy of the identification.

## REFERENCES

[1] J. Jung, S. Yoo, W. La, D. Lee, M. Bae, and H. Kim, “Avss: Airborne video surveillance system,” Sensors,
vol. 18, no. 6, p. 1939, 2018.

[2] S. Ren, K. He, R. Girshick, and J. Sun, “Faster r-cnn: Towards real-time object detection with region
proposal networks,” in Advances in neural information processing systems, 2015, pp. 91–99.

[3] Y. LeCun, Y. Bengio, and G. Hinton, “Deep learning,”nature, vol. 521, no. 7553, p. 436, 2015.

[4] C. Szegedy, W. Liu, Y. Jia, P. Sermanet, S. Reed, D.Anguelov, D. Erhan, V. Vanhoucke, and A. Rabinovich
“Going deeper with convolutions,” in Proceedings of the IEEE conference on computer vision and
pattern recognition, 2015, pp. 1–9.

[5] Dhumane, A., & Prasad, R. (2015). Routing challenges in internet of things. CSI Communications.

[6] Dhumane, A. V., Prasad, R. S., & Prasad, J. R. (2017). An optimal routing algorithm for internet of things enabling technologies. International Journal of Rough Sets and Data Analysis, 4(3), 1–16.