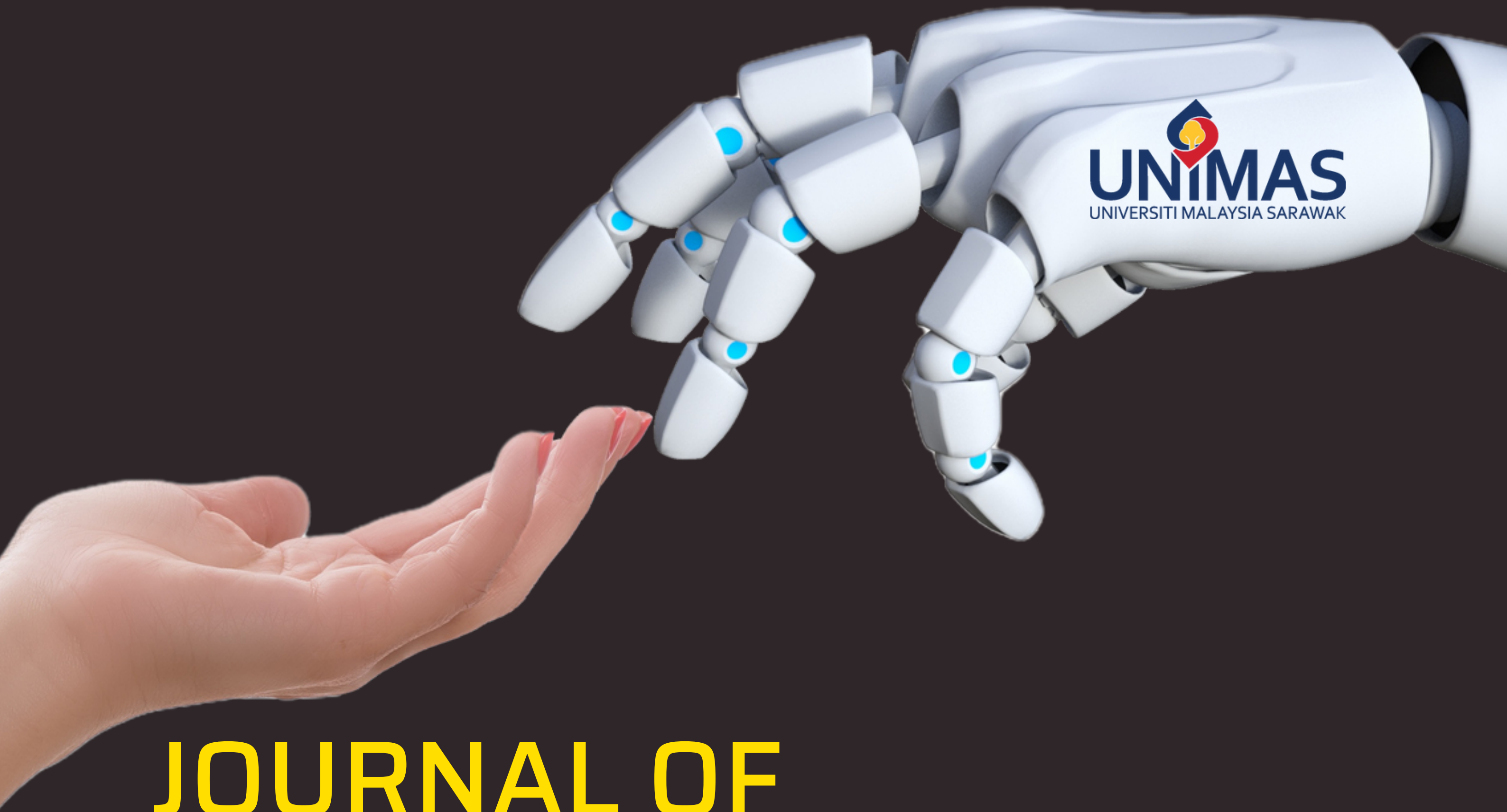


JOURNAL OF COMPUTING AND SOCIAL INFORMATICS

FACULTY OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY

UNIVERSITI MALAYSIA SARAWAK

eISSN 2821-3777

9 772821 377005

Editorial Committee

Advisory Board

Reviewers

Journal of Computing and Social Informatics

The Journal of Computing and Social Informatics (JCSI) is an international peer-reviewed publication that focuses on the emerging areas of Computer Science and the overarching impact of technologies on all aspects of our life at societal level. This journal serves as a platform to promote the exchange of ideas with researchers around the world.

Articles can be submitted via *www.jcsi.unimas.my*

Assoc Prof Dr Chiew Kang Leng

Chief Editor
Journal of Computing and Social Informatics
Faculty of Computer Science and Information Technology
Universiti Malaysia Sarawak
94300 Kota Samarahan
Sarawak, Malaysia

Contents

A Comparative Study of YOLOv5 and YOLOv7 Object Detection Algorithms

[1*]Oluwaseyi Ezekiel Olorunshola, [2]Martins Ekata Irhebhude and [3]Abraham Eseoghene Evwiekpaefe

[1]Electrical and Electronics Engineering Department, Air Force Institute of Technology, Kaduna,
[2,3] Computer Science Department, Nigerian Defence Academy, Kaduna, Nigeria

email: [1*]seyisola25@yahoo.com, [2]mirhebhude@nda.edu.ng, [3]aeevwiekpaefe@nda.edu.ng

**Corresponding author*

Received: 12 October 2022 | Accepted: 22 December 2022 | Early access: 08 February 2023

Abstract - *This paper presents a comparative analysis of the widely accepted YOLOv5 and the latest version of YOLO which is YOLOv7. Experiments were carried out by training a custom model with both YOLOv5 and YOLOv7 independently in order to consider which one of the two performs better in terms of precision, recall, mAP@0.5 and mAP@0.5:0.95. The dataset used in the experiment is a custom dataset for Remote Weapon Station which consists of 9,779 images containing 21,561 annotations of four classes gotten from Google Open Images Dataset, Roboflow Public Dataset and locally sourced dataset. The four classes are Persons, Handguns, Rifles and Knives. The experimental results of YOLOv7 were precision score of 52.8%, recall value of 56.4%, mAP@0.5 of 51.5% and mAP@0.5:0.95 of 31.5% while that of YOLOv5 were precision score of 62.6%, recall value of 53.4%, mAP@0.5 of 55.3% and mAP@0.5:0.95 of 34.2%. It was observed from the experiment conducted that YOLOv5 gave a better result than YOLOv7 in terms of precision, mAP@0.5 and mAP@0.5:0.95 overall while YOLOv7 has a higher recall value during testing than YOLOv5. YOLOv5 records 4.0% increase in accuracy compared to YOLOv7.*

Keywords: YOLOv5, YOLOv7, Object detection, Computer Vision, Detection Algorithm.

1 Introduction

There are several object detection algorithms such as Single Shot Detector (SSD), Region-based Convolutional Neural Network (R-CNN), and Fast Region-based Convolutional Neural Network (Fast R-CNN) (Padilla et al., 2021). In 2015, a researcher, Joseph Redmon, and colleagues introduced an object detection system that performed all the essential stages to detect an object using a single neural network. You Only Look Once (YOLO) is an object detection algorithm that detects various objects in a picture. It was founded in 2016. It reframes the object detection as a single regression problem, straight from image pixels to bounding box coordinates and class probabilities. This unified model predicts multiple bounding boxes and class probabilities simultaneously for those objects covered by boxes. At the time of its release, YOLO algorithm has produced impressive specifications that outstood the premier algorithms in terms of both speed and accuracy for detecting and determining object coordinates (Redmon, et al., 2016).

The base YOLO model processes images in real-time at 45 frames per second (FPS). A smaller version of the network: Fast YOLO, processes an astounding 155 FPS while still achieving double the mean Average Precision (mAP) of other real-time detectors. Compared to state-of-the-art detection systems, YOLO makes more localization errors but is less likely to predict false positives on background (Redmon et al., 2016).

YOLO algorithm can be used in wildlife, drones, military, autonomous driving, hospital, other Computer Vision (CV) tasks etc. (Górriz et al., 2020). Over the years, YOLO has developed many other variants such as YOLOv1, YOLOv2, YOLOv3, YOLOv4, YOLOv5, YOLOv6 and YOLOv7. However, there is need to evaluate which of the YOLO algorithms performs best of all the YOLO versions. From previous works, it was found that YOLOv5 performs better than previous YOLO versions (YOLOv3 and YOLOv4) in terms of accuracy and speed (Sahal, 2021; Ramya, et al., 2021) and the newly released version of YOLO which is YOLOv7 is also very performant. Hence, this study evaluated YOLOv5 and YOLOv7.

The rest of this paper is presented as follows; Section 2 briefly highlights the background of the YOLO, Section 3 reviews related works involving YOLOv5 and YOLOv7. Section 4 contains the methodology. Section 5 analyses and discusses the results, and finally, Section 6 details the conclusion of this study.

2 Background of YOLO

Redmon et al. (2016) presented YOLO, a new approach to object detection. The YOLO design enables end-to-end training and real-time speeds while maintaining high average precision. The system divides the input image into an S × S grid. If the center of an object falls into a grid cell, that grid cell is responsible for detecting that object. Each grid cell predicts B bounding boxes and confidence scores for those boxes. These confidence scores reflect how confident the model is that the box contains an object and also how accurate it thinks the box is that it predicts. Confidence is defined as the measure of the predicted object and the ground truth object. If no object exists in that cell, the confidence scores should be zero. Otherwise the confidence score should equal to the intersection over union (IOU) between the predicted box and the ground truth. Each bounding box consists of 5 predictions: x, y, w, h, and confidence. The (x, y) coordinates represent the center of the box relative to the bounds of the grid cell. The w and h are the width and height that are predicted relative to the whole image. Finally, the confidence prediction represents the IOU between the predicted box and the ground truth box.

The network architecture is inspired by the GoogLeNet model for image classification (Redmon et al., 2016). The network has 24 convolutional layers followed by 2 fully connected layers. Instead of the inception modules used by GoogLeNet, 1 × 1 reduction layers is utilized with a 3 × 3 convolutional layers. The YOLO architecture is shown in Figure 1.

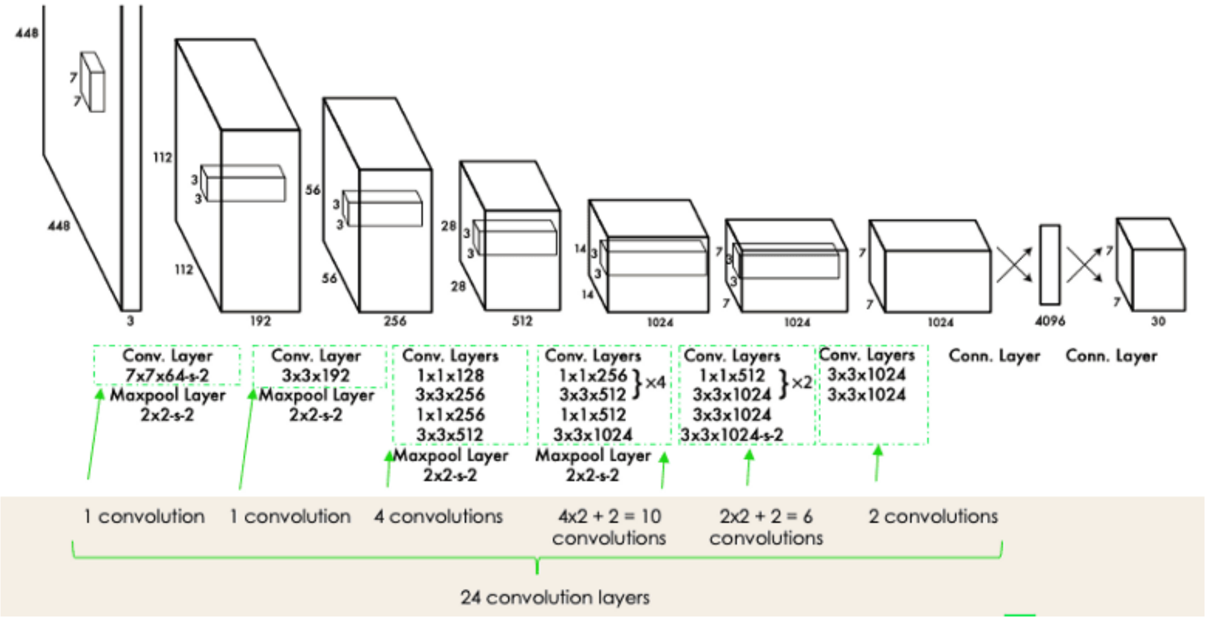


Figure 1: YOLO Architecture (Redmon et al., 2016)

Further improvements were made to the YOLO architecture as more research was done to improve detections by implementations of techniques and methods to improve accuracy, reduce the size of the network and offer faster detections. Such improvements are summarized in Table 1, while YOLOv5 and YOLOv7 are further discussed in the following subsections.

2.1 Improvements on YOLO Versions

From the introduction of the YOLO, there have been various changes and improvements which resulted in several versions of YOLO from YOLOv1 to YOLOv7. The findings on the YOLO versions are summarized in Table 1.

Table 1: Summary of Improvements on YOLO

S/N	YOLO Variant	Improvement	Results
1.	YOLOv1 (Redmon et al., 2016)	Single shot detector combines and solves the problem of drawing boundary boxes and class identification	Higher accuracy and speed compared to two-stage object detector such as Faster R-CNN
2.	YOLOv2 (Redmon & Farhadi, 2018)	Iterative improvements on Batch Normalization, higher resolution detection and use of anchor boxes	Reduction in architecture, faster detection and higher accuracy and better detection of high resolution images
3.	YOLOv3 (Redmon & Farhadi, 2018)	Addition of objectness score to bounding box prediction, added connections to the backbone network layers and predictions at three separate granularities.	Improves detection of smaller objects
4.	YOLOv4 (Alexey et al., 2020)	Improved feature aggregations, bag of freebies with mosaic augmentations and use of mish activation	Achieved improved accuracy and ease of training, high quality performance and accessibility
5.	YOLOv5 (Nepal & Eslamiat, 2022)	Reduced network parameters, use of Cross Stage Partial Network (CSPNet) for the head, PANet for the neck of the architecture, residual structure and auto-anchor. It also utilizes mosaic augmentations.	Extremely easy to train, inference on individual, batch images, video feed and webcam ports. Ease of transfer and use of weights. Faster and more lightweight than previous YOLO.
6.	YOLOv6 (Chuyi et al., 2022)	Redesigned network backbone and neck to EfficientRep Backbone and Rep-PAN Neck. The Network head is decoupled separating different features from the final head	Improvement in detecting small objects, anchor free training of model. Less stable and flexible as compared to YOLOv5.
7.	YOLOv7 (Wang et al., 2022)	Layer aggregation using E-ELAN, trainable bag of freebies, 35% fewer network parameters. Model scaling for concatenation-based model	Increase in speed and accuracy, ease of training and inference.

According to Nepal and Eslamiat (2022), the main differences between YOLOv1, YOLOv2, YOLOv3, YOLOv4, and YOLOv5 architecture are that YOLOv1 uses the softmax function, and YOLOv2 has higher resolution classifier, higher accuracy, and higher efficiency than YOLOv1. This is because batch normalization layer is added to the CNN of YOLOv2. YOLOv3 uses Darknet53 as its main backbone to extract features from the input image which has a better efficiency and detection performance. In YOLOv3, there is multi-object classification i.e. objects may belong to multiple categories at the same time. YOLOv3 replaces softmax function with an independent logistics function to calculate the probability that the input image belongs to a specific label and also YOLOv3 uses the 2-class entropy loss for each category thereby reducing the computational complexity brought about by softmax functions. YOLOv4 architecture uses CSPDarknet53 as a backbone which is a combination of Darknet53 and CSP network. YOLOv4 has higher accuracy, higher efficiency for object detection and also reduced hardware requirements. YOLOv5 uses Focus structure with CSPDarknet53 as a backbone. The Focus layer is first introduced in YOLOv5. The Focus layer replaces the first three layers in the YOLOv3 algorithm. The advantage of using a Focus layer is reduced required Compute Unified Device Architecture (CUDA) memory, reduced layer, increased forward propagation, and back propagation. YOLOv5 is extremely fast and is nearly 90% smaller (lighter) than YOLOv4. YOLOv6 has many improvements in backbone, neck, head and training strategies; YOLOv6 uses RepVGG Style structure, EfficientRep Backbone, Rep-PAN Anchor-free paradigm, SimOTA algorithm and SIoU bounding box regression loss function, while YOLOv7 exceeds all known object detectors in both speed and accuracy in the range from 5 FPS to 160 FPS, and has the highest accuracy 56.8% AP among all known real-time object detectors with 30 FPS or higher on GPU V100. YOLOv7 greatly improved real time object detection accuracy without increasing the inference cost, it reduced about 40% parameters and 50%

computation of state-of-the-art real-time object detector, and has faster inference speed and higher detection accuracy.

2.2 YOLOv5

A month after YOLOv4 was released, a researcher named Glenn, and his team, published a new version of the YOLO family, called YOLOv5. According to Nepal and Eslamiat (2022), YOLOv5 is different from the previous releases in that YOLOv5 utilizes PyTorch instead of Darknet. It utilizes CSPDarknet53 as backbone. It uses Path aggregation network (PANet) as neck to boost the information flow. PANet adopts a new feature pyramid network (FPN) that includes several bottom ups and top down layers. This improves the propagation of low level features in the model. PANet improves the localization in lower layers, which enhances the localization accuracy of the object. In addition, the head in YOLOv5 is the same as YOLOv4 and YOLOv3 which generates three different output of feature maps to achieve multi scale prediction. YOLOv5 model can be summarized as follows: Backbone: Focus structure, CSP network, Neck: SPP block, PANet, Head: YOLOv3 head using GIoU-loss. The improvement of YOLOv5 over YOLOv4 was utilization of CSPDarknet53 which solved the problem of repetitive gradient information found in YOLOv4 and YOLOv3 thereby reducing the network parameters and reducing inference speed while accuracy is increased. The architecture of YOLOv5 is shown in Figure 2.

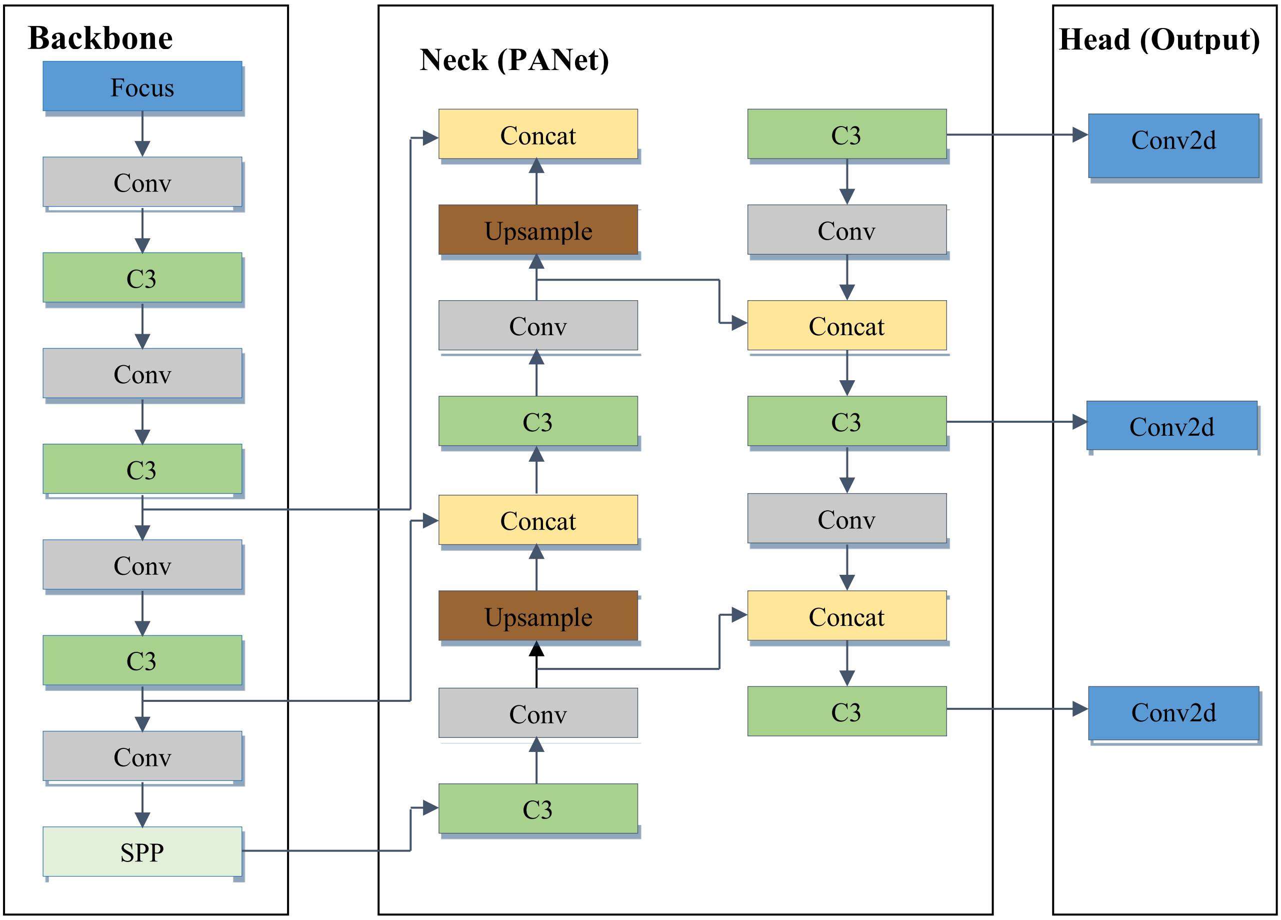
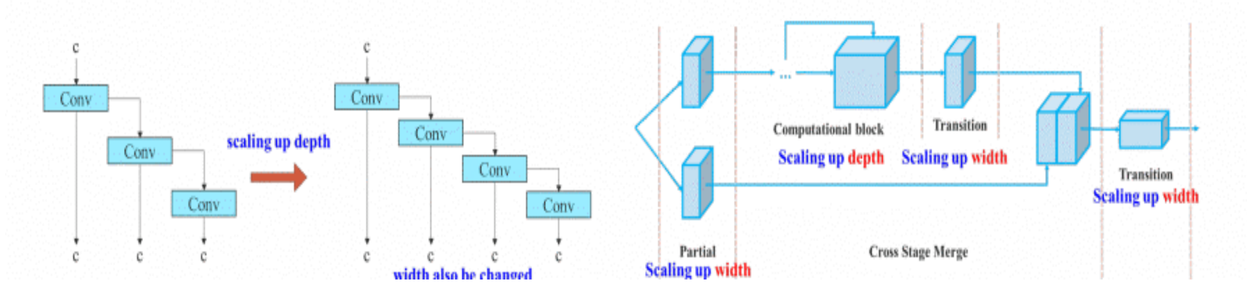


Figure 2: YOLOv5 Architecture (Nepal & Eslamiat, 2022)

2.3 YOLOv7

YOLOv7 is the latest version of the YOLO at the time of this research. YOLOv7 is a real-time object detector currently revolutionizing the CV industry with its incredible features. YOLOv7 was trained only on MS COCO dataset from scratch without using any other datasets or pre-trained weights (Wang et al., 2022). Wang et al. (2022) stated that YOLOv7 surpasses all known object detectors in both speed and accuracy in the range from 5 FPS to 160 FPS, and has the highest accuracy at 56.8% AP among all known real-time object detectors with 30 FPS or higher on Graphics Processing Units (GPU) V100. YOLOv7 greatly improved real time object detection accuracy without increasing the inference cost; it reduced about 40% parameters and 50% computation of state-of-the-art real-time object detector, and has faster inference speed and higher detection accuracy.

YOLOv7 has extended efficient layer aggregation networks (E-ELAN). E-ELAN uses expand, shuffle, and merge cardinality to achieve the ability to continuously enhance the learning ability of the network without destroying the original gradient path (Wang et al. 2022). E-ELAN only changes the architecture in computational block, while the architecture of transition layer is completely unchanged. In addition to maintaining the original E-LAN design architecture, E-ELAN also guides different groups of computational blocks to learn more diverse features. YOLOv7 also has model scaling for concatenation-based models. The main purpose of model scaling is to adjust some attributes of the model and generate models of different scales to meet the needs of different inference speeds. Proposed compound scaling method can maintain the properties that the model had at the initial design and maintains the optimal structure. Figure 3 is the Model scaling for concatenation-based models of YOLOv7.



(a) concatenation-based model (b) scaled-up concatenation-based model (c) compound scaled up depth and width for concatenation-based model

Figure 3: Model Scaling of YOLOv7 (Wang et al., 2022)

From (a) to (b), it is observed that when depth scaling is performed on concatenation-based models, the output width of a computational block also increases. This phenomenon will cause the input width of the subsequent transmission layer to increase. Therefore, (c) is proposed, that is, when performing model scaling on concatenation-based models, only the depth in a computational block needs to be scaled, and the remaining of transmission layer is performed with corresponding width scaling.

YOLOv6 also offers great improvements in terms of detection but lacks scalability and ease of training when compared with YOLOv5 and YOLOv7. Also, YOLOv6 performs more accurately when used for single image inference compared to multiple image inference accuracy offered by YOLOv5 and YOLOv7 (Banerjee, 2022). As a result of this, experiment was conducted with YOLOv5 and YOLOv7 as they fit in for the multiple object detection, providing ease in customizing the training and running of inference.

3 Literature Review

Kasper-Eulaers et al. (2021) studied how YOLOv5 can be implemented to detect heavy goods vehicles at rest areas during winter to allow for the real-time prediction of parking spot occupancy. The model was trained using Google Colaboratory (Colab), which provides free access to powerful GPUs and requires no configuration. A notebook was developed by Roboflow.ai which is based on YOLOv5 and uses pre-trained COCO weight. The model improved swiftly in terms of precision, recall and mean average precision before overfitting after about 150 epochs. The box, objectness and classification losses of the validation data also showed a rapid decline until around epoch 15. Results show that the trained algorithm can detect the front cabin of heavy goods vehicles with high confidence, while detecting the rear seems more difficult, especially when located far away from the camera.

Malta et al. (2021) proposed a model of a task assistant based on a deep learning neural network. A YOLOv5 network was used for recognizing some of the constituent parts of an automobile. The dataset created consisted of 582 images taken from three videos with similar lighting conditions, where it was possible to identify a total of eight different types of parts: oil dipstick; battery; engine oil reservoir; wiper water tank; air filter; brakes fluid reservoir; coolant reservoir; and power steering reservoir. The images taken from each frame were converted to a 416 × 416 format, which is the format that the chosen architecture needs to use as input. The hardware used during development included computers, for running software, and cell phones, for capturing videos and pictures. The object detection model was trained using laptop computer with access to a Google Colab virtual machine. The precision obtained for the two models (YOLOv5s and YOLOv5m) was in line with that obtained by other authors for similar problems. YOLOv5s demonstrated to be capable of identifying eight different mechanical parts in a car engine with high precision and recall always above 96.8% in the test sets, which, compared to the larger model, has almost the same results. Results proved that the network is good and fast enough to be applied to the task of assisting in recognizing constituent parts of an automobile.

Wan et al. (2021) proposed a YOLOv5 model based on a self-attention mechanism for polyp target detection. Mosaic method was used in the data preprocessing stage to enhance the amount of training data in the data set, Cross Stage Partial Networks (CSPNet) was used as the backbone network to extract the information features in the image, which solved the problem of gradient disappearance, and the feature pyramid architecture with attention mechanisms was used to enhance the detection performance of varying-size polyps. The proposed method was trained by stochastic gradient descent (SGD) and backpropagation in an end-to-end way on a cloud-computing platform configured with eight 16 GB GPUs, a 16-core CPU, and a 64 GB memory. YOLOv5 used spatial pyramid pooling (SPP) to enhance the model's detection of objects with different scales, Path aggregation network (PANET) as the neck for feature aggregation and new Feature Pyramid Networks (FPN) structure that enhanced the bottom-up path, which improved the propagation of low-level features. The author's method achieved excellent performance. In the Kvasir-SEG data set, the precision was 0.915, the recall rate was 0.899 and the F-score was 0.907. In the WCY data set, the precision was 0.913, the recall was 0.921 and the F-score was 0.917. Specifically, this method used full-image information when predicting the target window using each network, which greatly reduced the false positive rate.

Yao et al. (2021) developed a defect detection model based on YOLOv5, which is able to detect defects accurately, and at a fast speed. A small object detection layer was added to improve the model's ability to detect small defects. Squeeze-and-Excitation (SE) Layer and the loss function complete intersection over union (CIoU) were introduced to make the regression more accurate. The model was trained based on transfer learning and used the Cosine Annealing algorithm to improve the effect. The mAP@0.5 of YOLOv5 reached 94.7%, which was an improvement of nearly 9%, compared to the original algorithm.

Jia et al. (2021) introduced a real-time end-to-end helmet detection of motorcyclists method based on YOLOv5 algorithm. The original anchor box size of YOLOv5 is calculated by the K-means algorithm in the COCO dataset, and the HFUT-MH dataset proposed is quite different from the COCO dataset. This method achieved mAP of 97.7%, F1-score of 92.7% and frames per second of 63, which outperformed other state-of-the-art detection methods.

In Liu et al. (2021), a real time railway signal lights detection based on YOLOv5 was introduced. Experiments were conducted to prove the effectiveness of the proposed method. A dataset consisting of subway scenes with signal lights was constructed, and trained with YOLOv5 model. The signal lights detection model trained by YOLOv5s has an average recall rate and accuracy of 0.972, while running speed reached 100 FPS.

Patel et al. (2022) proposed an ensemble model for translated infrared images. The model uses advanced deep learning models which are pix2pix Generative Adversarial Networks (GAN) and YOLOv7 on the LLVIP dataset which contains visible-infrared image pairs for low light vision. The dataset amounting to 33672 images mostly captured in dark scenes and tightly synchronized with time and location. The model was able to outperform models trained with just images against the translated images in all aspects especially conditions of low light. The model has higher precision, recall, mAP@0.5 and mAP@0.5:0.95 for translated images than for visible images which was graphically represented.

Dima et al. (2021) proposed a YOLOv5 based solution because of its lightweight, good speed and accuracy. MU HandImages ASL, which is a benchmark dataset, was used to train and evaluate the model. The data set contains 2515 close-up, colored images. Authors achieved 95% precision, 97% recall, 98% map@0.5, and 98% map@0.5:0.95 score which is adequate to recognize the gesture in real-time. The achieved results, even with a relatively small data set, are on average 0.98 F1 scores in the identification of 36 distinct classes of ASL. This result indicates a good potential for using YOLOv5 to recognize the ASL dataset.

Hao et al. (2021) proposed a lightweight algorithm which improves YOLOv5 in both speed and accuracy. The model was experimented with dataset containing fire scenarios and shows that the Light-YOLOv5 improves mAP by 3.3% and achieves FPS of 91.1. Compared with YOLOv7-tiny, the mAP of the improved model was 6.8% higher, which shows how effective the algorithm is.

Cengil and Cinar's (2021) study aimed to identify poisonous mushrooms. YOLOv5 was used in real-time applications due to its speed and high accuracy rate. It is also good at finding small objects. Mean Average

Precision of all classes was 0.77 and AP values of each class were 0.818 for Autumn Skullcap, 0.825 for Destroying Angle, 0.610 for Cococybe Filaris, 0.737 for Deadly Dapperling, 0.826 for Death Cap, 0.854 for Podostroma Cornu-Damae, 0.993 for Fly Agaric, 0.556 for Webcaps. The experimental results showed that with the image data used, a high success rate was achieved.

Yang et al. (2022) added YOLOv7 as object detection network to DeepSORT tracking algorithm to get YOLOv7-DeepSORT detection by tracking model. The evaluation metrics used in the experiment were: Multiple Object Tracking Accuracy (MOTA), Multiple Object Tracking Precision (MOTP), Identity F1 Score (IDF1), Number of Identity Switches (IDs), Mostly Lost Targets (ML), Mostly Tracked Targets (MT), False Positive (FP), and False Negative (FN). Experiments showed that YOLOv7 gave higher scores than YOLOv5 in MOTA, MOTP and IDF1. For IDs, ML, MT, FP and FN, it was reported that YOLOv5 is better than YOLOv7.

Hussain et al. (2022) presented a CV-based autonomous rack inspection framework centered around YOLOv7 architecture to solve the problem of manual process results in operational down-time as well as inspection and certification costs and undiscovered damage due to human error. Additionally, the authors proposed a domain variance modeling mechanism for addressing the issue of data scarcity through the generation of representative data samples. The proposed framework achieved a mAP of 91.1%.

YOLOv7 is a recent model of the YOLO variant. From the reviews, authors that have conducted comparison on the use of YOLOv7 reported significant improvement in performance when compared with other variants. To investigate and clearly confirm the improvement and performance of the YOLOv7, an experiment was conducted to compare and clearly identify the performance of both models: YOLOv5 and YOLOv7, for effective training and subsequent application as the detection model. Table 2 contains the summary of the literature reviewed in the course of this research.

Table 2: Summary of Literature Review

Authors/Date	Methodology	Analysis & Results	Conclusions
Kasper-Eulaers et al. (2021)	Real Time detection of heavy-duty vehicles for occupancy of parking spot suing YOLOv5	Improvement on precision, recall and mAP in detection. The model was able to detect front cabin with high confidence but fails when located at a far distance.	The model shows improvement on close range detection, but at a far distance, shows poor detection.
Malta et al. (2021)	Recognition of different constituents of a car using YOLOv5 series.	The model was able to achieve precision and recall of 96.8% in detection of the eight parts of the car engine used in the experiment compared with larger models used for the same purpose.	The experiment compares that the smaller models could perform in terms of precision and recall a high value compared with larger models while still offering speed due to size of the model.
Wan et al. (2021)	Experiment using YOLOv5 model for self-attention mechanism for polyp target detection.	The model was able to achieve excellent recall, precision and accuracy of above 90% due to the use of full image information during prediction in each network.	The use of full image information in each network of a model can enhance the model in detection and lower the rate of false positives.
Yao et al. (2021)	Experiment of defect detection using YOLOv5 with addition	The model achieved a mAP@0.5 of 94.7% which improved the model	Addition of a small detection layer like the SE layer can improve the model detection while also offering faster detection.

	of a Squeeze-and-Excitation (SE) layer.	by 9% compared to the original model	
Jia et al. (2021)	A real-time end to end helmet detection of motorcyclists using YOLOv5 using K-means algorithm to calculate the anchors	The model achieved 97.7% mAP and 92.7% F1 scores which outperforms other state-of-the-art models	Use of well calculated anchors can greatly improve model detection.
Patel et al. (2022)	An ensemble model proposed for translated infrared images using pix2pix, GAN and YOLOv7 on visible infrared image pairs for low light visiowhns	The model performed better when compared with just images used for training as against the model use of translated images especially on low light conditions.	The use of translated images can improve the accuracy of a model especially on low light condition and also ensemble model of good algorithms can also perform better than an original detection model algorithm
Hao et al. (2021)	Experiment with YOLOv5 combined with a light weight algorithm was compared with YOLOv7-tiny in fire scenarios	The model improved by 6.8% compared with YOLOv7-tiny with improvements on mAP and FPS.	Light weight algorithms can prove to be effective in speed and accuracy when combined with state-of-the-art algorithms
Yang et al. (2022)	Experiments to compare YOLOv5 and YOLOv7 in terms of tracking using different evaluation metrics	The results showed that YOLOv7 performed better in some of the evaluation metrics such as MOTA, MOTP and IDF1 while YOLOv5 outperformed YOLOv7 in IDs, ML, MT, FP and FN.	Both algorithms showed good results in tracking experiment. The evaluation metrics of choice in an experiment will decide which of the models to consider for implementation.
Hussain et al. (2022)	A CV-based autonomous rack inspection framework using YOLOv7 and a domain variance modeling mechanism for addressing data scarcity.	The model achieved mAP of 91.1%	The model automated the process. Human errors due to undiscovered damage were reduced.

4 Methodology

Experiments were carried out by training custom datasets model with both YOLOv5 and YOLOv7 independently in order to consider which one of the two performs better in terms of precision, recall, mAP@0.5 and mAP@0.5:0.95 as these metrics determine which one performs better in terms of overall detection. For the quantitative analysis of the models, the metrics used are explained as follows:

i. Precision measures the proportion of accurately categorized positive samples (True Positive) to the total number of positively classified sample (either correctly classified or not, True Positive + False Positive).
ii. The recall value is calculated by taking ration of True Positive to all Positive samples (True Positive + False Negative). It measures how well the model can identify positive samples.
iii. The mAP@0.5 calculates a score by comparing the detected box to the ground-truth box bounding box at IoU threshold of 0.5. The model's detections are the more precise, the higher the score.
iv. mAP@0.5:0.95 refers to the average mAP over various thresholds, from 0.5 to 0.95, in steps of 0.05.

4.1 Experiment Setup

Google Colab which is a platform that offers free coding notebook, a cloud virtual machine with storage, a GPU and Tensor Processing Unit (TPU) for running long and complex computing was used for the experiment on the detection models. All experiments were conducted on HP Probook 6570b using Google Chrome browser to access Google Colab for running the training, validation and the testing of the custom model. The results of the training, validation and testing were saved on Google Drive which can be loaded for further use. The platform is Linux-based (Linux OS) with access to all resources a physical computer possesses. The platform also allows access to the Google drive which is important for loading in the dataset and saving the files.

4.2 Dataset Description

The dataset used in this experiment were Google Open Images Dataset (Google Open Images, n.d.), Roboflow Public Dataset (Roboflow, n.d.) and locally sourced images. Primarily, the images gotten from Google Open Images, which is a large-scale dataset with different trainable classes, were a total of 5808 and they comprise Person, Handgun, Rifle and Knife classes. A total of 2971 images of Pistols were also gotten from Roboflow Public Dataset and modified to class "Handgun" and added to the dataset to make a total of 8779 images. Added to the dataset were locally sourced images from different military theatres of operation. The locally sourced images consist of about 1000 images which captured various persons, handguns, pistols, rifles and knives of different types using a high-definition D5100 DSLR Nikon camera. The camera was set to capture images in resolution of 1280 x 720 pixels which is the resolution used by YOLOv7 and YOLOv5. The images were gathered, cleaned and annotated as Person, Handgun, Rifle and Knife classes using Roboflow Annotation tool. Data preprocessing done on the dataset was Auto-Orient and the images were resized to 416 x 416 (weight x height) size which is the size used by both YOLOv5 and YOLOv7. The dataset used for the training were 9779 images containing 21,561 annotations of the four classes. The dataset was split into training, testing and validation on ratio 60:20:20 of the number of images annotated. 5867 images which makes up 60% of the dataset was used for training while 1955 images which makes up 20% of the total images was used for testing and 1955 images which amounts to 20% of the total images remaining was used for validation. Figure 4 shows the sample images of the dataset gotten from Google Open Images Dataset (left), Roboflow Public Dataset (centre) and locally sourced images (right).

Figure 4: Sample images of the dataset used in the research.

5 Results and Discussion

The output values of the performance results gotten from testing of YOLOv7 model and YOLOv5 model are shown in Table 2.

Table 2: Performance Result of YOLOv7 and YOLOv5

Class	Images	Precision		Recall		mAP@0.5		mAP@0.5:0.95	
		YOLOv7	YOLOv5	YOLOv7	YOLOv5	YOLOv7	YOLOv5	YOLOv7	YOLOv5
All	1767	0.528	**0.626**	**0.564**	0.534	0.512	**0.553**	0.315	**0.342**

Handgun	1767	0.778	**0.819**	0.778	**0.785**	0.814	**0.829**	0.584	**0.599**
Knife	1767	0.588	**0.716**	**0.746**	0.695	0.669	**0.740**	0.431	**0.488**
Person	1767	0.382	**0.511**	**0.524**	0.410	0.380	**0.398**	0.173	**0.181**
Rifle	1767	0.363	**0.458**	0.209	**0.247**	0.183	**0.242**	0.0735	**0.101**

5.1 Precision

For precision, comparing the results of YOLOv7 and YOLOv5 from Table 2, it can be seen that YOLOv5 outperforms YOLOv7 in all cases. YOLOv5's all classes had 62.6% and 81.9%, 71.6%, 51.1% and 45.8% for Handgun, Knife, Person and Rifle classes respectively compared with YOLOv7 having 52.8% for all classes, 77.8%, 58.8%, 38.2% and 36.3% respectively for Handgun, Knife, Person and Rifle classes respectively. From the comparison, YOLOv5 has more true positives to total number of detected objects compared YOLOv7 by 9.8% difference in overall class detection. Both models have more detection for the class of Handgun compared to other classes with a difference of 4% when compared with YOLOv7. The model in this case will efficiently identify Handgun more than the other classes.

5.2 Recall

For the results of recall in Table 2, it can be seen that YOLOv5 outperforms YOLOv7 in only Handgun and Rifle detection with results of 78.5% and 24.7% compared with YOLOv7 results of 77.8%, 20.9%. For the overall class recall, Knife and Person, YOLOv7 outperforms YOLOv5 with YOLOv7 having 56.4%, 74.6%, 52.4% compared with YOLOv5 having 53.4%, 69.5% and 41%. For the recall value, Handgun mostly recalled during detection with a percentage of 78.5% for YOLOv5 compared with 77.8% of YOLOv7 with a slight difference of 0.7%. YOLOv7 in this case was able to surpass YOLOv5 in identifying the Knife and the Person classes making an overall class recall better than YOLOv5 with a slight difference of 3%. Meanwhile, YOLOv5 also has better recall in Handgun and Rifle class detection compared to YOLOv7.

5.3 Accuracy in Terms of mAP@0.5 and mAP@0.5:0.95

For mAP@0.5 and mAP@0.5:0.95, comparing the results in Table 2, it is seen that YOLOv5 gave a better result in terms of accuracy than YOLOv7 in all cases, with the overall class results in mAP@0.5 and mAP@0.5:0.95 of 55.3% and 34.2% compared with 51.2% and 31.5% of YOLOv7. The mAP values comparing the detected box to the ground truth bounding box at IOU of 0.5 shows that the model precise detection of an object in a frame. With YOLOv5 having mAP@0.5 of 4% difference compared with that of YOLOv7 shows how well the model is able to rightly and accurately detect objects when compared with the ground truth objects. With average mAP at different thresholds the mAP@0.5:0.95 also records better performance for YOLOv5 compared with YOLOv7 with a slight difference of 2.7%.

It is observed that the YOLOv5 model performs better than YOLOv7 for all the performance metrics except for the case of recall score during testing. It is deduced from the experiments that YOLOv5 has better detection accuracy, precision and less recall than YOLOv7 especially when used during production as deduced from the testing results.

6 Conclusion

This paper conducted a comparative analysis of the widely used YOLOv5 and the relatively new YOLOv7. The experiment carried out shows significant contribution compared to other works earlier mentioned in the literature review. It shows the ease of setting up and use of detection models, and the use of the different evaluation metrics for the experimentation for comparison. The experiment also demonstrates the effectiveness of the YOLOv5 model compared with YOLOv7. These two versions of YOLO were compared in terms of precision, recall, and mAP. It is observed from the experiment conducted that YOLOv5 gave a better result than YOLOv7. YOLOv5 gave a precision value of 62.6% compared to 52.9% of YOLOv7, accuracy score of 55.3% to 51.2%, while YOLOv7 has slightly higher recall than YOLOv5 during testing. Also, YOLOv5 outperformed YOLOv7 in mAP@0.5:0.95. The experiment performed showed better performance in favour of YOLOv5. The results from the experiment will benefit researchers seeking to use either one of the models as a reference for choice of experiment by considering the evaluation metrics. However, with more research on both models, clear performance difference will be pointed out clearly, as one model may perform better than other in different applications and use cases.

References

Alexey B., Chien-Yao W., Hong-Yuan M. L. (2020) Yolov4: Optimal speed and accuracy of object detectionarXiv:2004.10934.

Banerjee A. (2022). *YOLOv5 vs YOLOv6 vs YOLOv7*. Retrieved October 12, 2022, from https://www.learnwitharobot.com/p/yolov5-vs-yolov6-vs-yolov7/.

Cengil, E., & Cinar, A. (2021). Poisonous mushroom detection using YOLOV5. *Turkish Journal of Science and Technology*, *16*(1), 119-127.

Chuyi L., Lulu L., Hongliang J., Kaiheng W., Yifei G., Liang L., Zaidan K., Qingyuan L., Meng C., Weiqiang N., Yiduo L., Bo Z., Yufei L., Linyuan Z., Xiaoming X., Xiangxiang C., Xiaoming W., Xiaolin W. (2022). YOLOv6: A single-stage object detection framework for industrial applications. _arXiv_:2209.02976

Dima, T. F., & Ahmed, M. E. (2021, July). Using YOLOv5 Algorithm to Detect and Recognize American Sign Language. In *2021 International Conference on Information Technology (ICIT)* (pp. 603-607). IEEE.

Google Open Images. (n.d.). Google Open Images Dataset of Person, Handgun, Rifle and Knife. Retrieved from https://storage.googleapis.com/openimages/web/visualizer/index.html.

Górriz, J. M., Ramírez, J., Ortíz, A., Martínez-Murcia, F. J., Segovia, F., Suckling, J. & Ferrández, J. M. (2020). Artificial intelligence within the interplay between natural and artificial computation: Advances in data science, trends and applications. *Neurocomputing*, *410*, 237-270.

Hao, X., Bo, L., & Fei, Z. (2021). Light-YOLOv5: A Lightweight Algorithm for Improved YOLOv5 in Complex Fire Scenarios.

Hussain, M., Al-Aqrabi, H., Munawar, M., Hill, R., & Alsboui, T., (2022). Domain Feature Mapping with YOLOv7 for Automated Edge-Based Pallet Racking Inspections. *Sensors, 22, 6927.*

Jia, W., Xu, S., Liang, Z., Zhao, Y., Min, H., Li, S., & Yu, Y. (2021). Real-time automatic helmet detection of motorcyclists in urban traffic using improved YOLOv5 detector. *IET Image Processing*, *15*(14), 3623-3637.

Kasper-Eulaers, M., Hahn, N., Berger, S., Sebulonsen, T., Myrland, Ø. & Kummervold, P. E. (2021). Detecting heavy goods vehicles in rest areas in winter conditions using YOLOv5. *Algorithms*, *14*(4), 114.

Liu, W., Wang, Z., Zhou, B., Yang, S., & Gong, Z. (2021, May). Real-time signal light detection based on yolov5 for railway. In *IOP Conference Series: Earth and Environmental Science* (Vol. 769, No. 4, p. 042069). IOP Publishing.

Malta, A., Mendes, M., & Farinha, T. (2021). Augmented reality maintenance assistant using yolov5. *Applied Sciences*, *11*(11), 4758.

Nepal, U., & Eslamiat, H. (2022). Comparing YOLOv3, YOLOv4 and YOLOv5 for Autonomous Landing Spot Detection in Faulty UAVs. *Sensors*, *22*(2), 464

Padilla, R., Passos, W. L., Dias, T. L., Netto, S. L., & da Silva, E. A. (2021). A comparative analysis of object detection metrics with a companion open-source toolkit. Electronics, 10(3), 279.

Patel, D., Patel, S., & Patel, M. (2022). Application to image-to-image translation in improving pedestrian detection.

Ramya, A., Venkateswara, G. P., Amrutham, B.V., Sai, S. K. (2021). Comparison of YOLOv3, YOLOv4 and YOLOv5 Performance for Detection of Blood Cells. *International Research Journal of Engineering and Technology (IRJET) 8(*4*),* (pp. 4225 – 4229).

Redmon, J., Divvala, S., Girshick, R., & Farhadi, A. (2016). You only look once: Unified, real-time object detection. In *Proceedings of the IEEE conference on computer vision and pattern recognition* (pp. 779-788).

Redmon, J., & Farhadi, A. (2018). Yolov3: An incremental improvement. *arXiv preprint arXiv:1804.02767*.

Roboflow (n.d). Roboflow Public Dataset (n.d). Public Dataset of Pistols. Retrieved from https://public.roboflow.com/object-detection/pistols

Sahal, M. A. (2021). Comparative Analysis of Yolov3, Yolov4 and Yolov5 for Sign Language Detection. *IJARIIE, 7*(4), (pp. 2395 – 4396).

Wan, J., Chen, B., & Yu, Y. (2021). Polyp Detection from Colorectum Images by Using Attentive YOLOv5. *Diagnostics*, *11*(12), 2264.

Wang, C. Y., Bochkovskiy, A., & Liao, H. Y. M. (2022). YOLOv7: Trainable bag-of-freebies sets new state-of-the-art for real-time object detectors. *arXiv preprint arXiv:2207.02696*.

Yang, F., Zhang, X., & Liu, B. (2022). Video object tracking based on YOLOv7 and DeepSORT. *arXiv preprint arXiv:2207.12202*.

Yao, J., Qi, J., Zhang, J., Shao, H., Yang, J., & Li, X. (2021). A real-time detection algorithm for Kiwifruit defects based on YOLOv5. *Electronics*, *10*(14), 1711.

Awareness of National Cyber Security Weaknesses Due to Cyber-Attacks Through the Use of UAV

[1*]Muhammad Quazy Bin Razali, [2]Adnan Shahid Khan, [3]Shalin Binti Shaheezam Khan and [4]Aruen Anak Manggau

[1]Jabatan Imigresen Malaysia, Negeri Sarawak, Aras 1, Bangunan Sultan Iskandar, Jalan Simpang Tiga, 93550 Kuching, Sarawak, Malaysia
[2, 3, 4]Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak, 94300 Kota Samarahan, Sarawak, Malaysia

email: [1*]muhammad_quazy@imi.gov.my, [2]skadnan@unimas.my [3]21030393@siswa.unimas.my, [4]21030394@siswa.unimas.my

*Corresponding author

Received: 04 September 2022 | Accepted: 14 March 2023 | Early access: 06 April 2023

Abstract - *Unmanned Aerial Vehicle (UAV) is a utility tool created to provide a simple task and provide an important impact in matters of national defence, especially on the military side to monitor terrorists in camp areas and also on the borders of the country, to preserve the well-being and prosperity of the people in our country is always guaranteed. However, UAVs have been misused by certain parties to fulfil their interests. This lack of integrity in the use of UAV equipment should be curbed so that it does not continue with proper disclosure and understanding. Every day, various issues arise due to the misuse of technology, which will affect society and the country. Therefore, the government is making every effort to deal with the problem because the limited awareness of the use of UAVs is very worrying, especially the monitoring from the authorities. The authorities should also play an important role in enacting regulations and laws against those who misuse these UAV devices.*

Keywords: Awareness, Unmanned Aerial Vehicle, Cyber Security, Threats, Responsibilities.

1 Introduction

Unmanned aerial vehicles (UAVs) are being used more and more every day. Now there are many models of UAVs because of demands for monitoring work for organizations such as agriculture, development, military, network services, traffic control, real estate, delivery of medical supplies and so on in facilitating business using UAV tools (Gromada & Stecz, 2021). Nevertheless, there are a few irresponsible parties who misuse UAV equipment for other uses such as espionage which can disturb the peace and privacy of other individuals, leading to sexual harassment more extreme at the moment, hacking such equipment is becoming more and more common. This matter should be given attention by the authorities by enacting new regulations and laws to deal with this non-permanent problem (Pan et al., 2022).

Various new models of UAVs are being created and marketed according to the demands of specific users or organizations in addition to current technology specifications. The market value of UAVs also depends on the quality of the features found on the vehicle, the more sophisticated the features found in the use of the UAV, the higher the market value, and it also depends on the size of the design and the ability of the UAV to bear the load carried. These UAVs are common in other countries where they are used as a service to deliver supplies to those living in high-rise apartment buildings (Asghar Khan et al., 2022).

Therefore, with the availability of UAV technology, those who use it should have adequate awareness to avoid misuse. Nowadays, it is more about the parties' understanding of the use of these UAVs for cyber security (Haider et al., 2022). The authorities must take various steps before the organization owns this UAV. They should know more about it, for example, place a license on the owner of this UAV. Although it looks like a machine, this UAV

does not have a driver but is controlled using various types of remote-control devices which can lead to misuse of the UAV (Wu et al., 2022). We can see in the diagram below an example of a basic UAV control.
In the current technology of IoT and Industry 4.0, UAV is a network that gathers data from IoT devices in other words, it has been implemented into one of today's technology networks, namely Green IoT and B5G (Beyond 5G) at the same time it makes the world smarter in crossing the telecommunications network, therefore this truth has been explained through the article "Ad Hoc Network" which describes how UAVs are used in today's network services (Tomaszewski et al., 2022; Alsamhi et al., 2021).

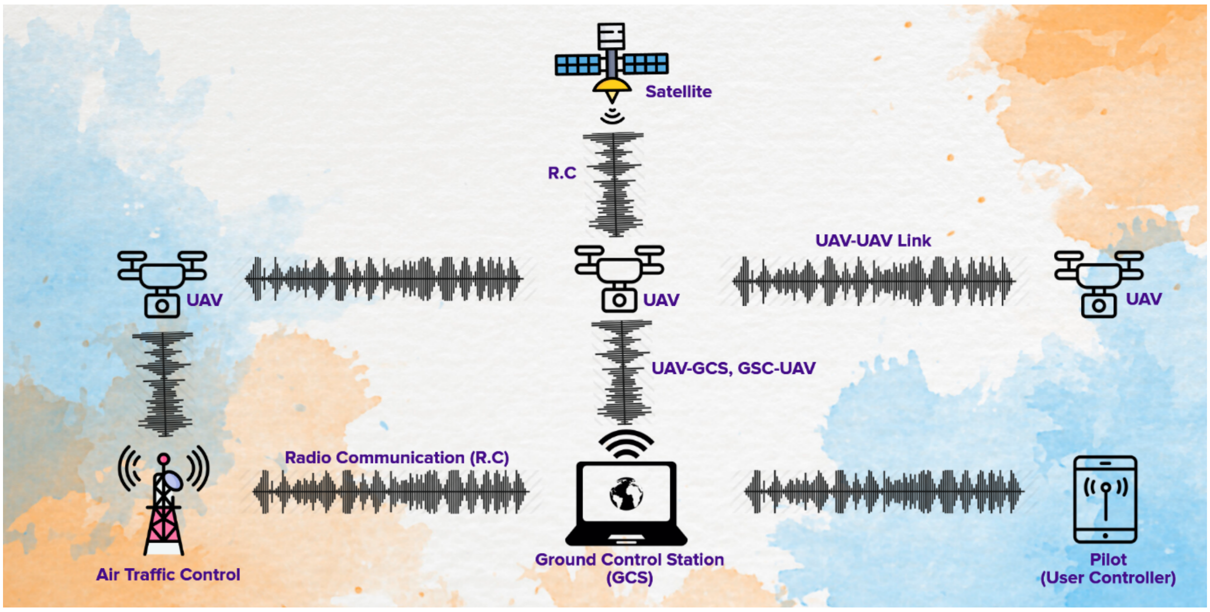


Figure 1: Basic and generic architecture of UAV

The rest of the paper is organized as follows: The abstract is in the first part and Section 1 provides a brief introduction to Unmanned Aerial Vehicle's general overview. Section 2 discusses the literature review which includes a summarization of 10 articles. Section 3 discusses the taxonomy of technology from perspectives of attacks and techniques used to mitigate attacks. Section 4 elaborates on research trends, and challenges faced by this technology and predicts future research directions. Finally, conclusions are made in Section 5 followed by acknowledgement and references.

2 Literature Review

Alrefaei et al. (2022) examine the effects of UAV wireless network's jamming and spoofing assault as well as the earlier traditional security detection and defensive mechanisms. It also discusses the advantages of deep learning technology and demonstrates how it may be used to safeguard UAV networks. The UAV demonstrates its adaptability to usage and application for various tasks. The performance of the UAV system degrades due to threats that might affect natural UAV communication connections. The adversary discovered that it is simple to carry out their easy task by listening to the transmission data. This article discusses several assault defence strategies and threat detection methods.

This study suggests BISSIAM, a unique framework that can recognise UAVs' existence, varieties, and operational modes (Li et al., 2021) this sentence is incomplete. A sampling procedure is provided to maximise the training sample size without sacrificing model correctness or training effectiveness. Also, to detect unseen UAVs without retraining the entire model, developing a similarity-based fingerprint-matching approach this sentence is incomplete. The results of the experiments demonstrate that the method beats existing baselines and can detect UAVs with 92.85% accuracy in unsupervised learning settings.

Li et al. (2020) discuss physical layer security problems in unmanned aerial vehicles (UAVs) communication networks. An iterative technique is suggested to achieve this goal by simultaneously optimising the trajectory and transmit power of the two UAVs. Simulation results show that, compared to the standards, the suggested system may significantly increase secrecy rates. Simulations showed that the suggested optimization technique presents

more desirable flying trajectories compared to the benchmarks and may greatly increase the system secrecy rate performance.
In the article by Abhishek et al. (2022), UAV-aided networks introduced the Malicious Aerial Vehicle Detection (MaDe) lightweight data integrity preservation technique. Every sensor in MaDe periodically sends out a feedback packet. MaDe will spot any UAV tampering with the packets which carry authentication on each packet sent or received by the sensor and base station. None of these computationally intensive cryptographic methods is used to do this. MaDe delivers much lower overhead and latency than existing techniques, according to communication overhead and latency measurements. The outcomes demonstrate MaDe's exceptional effectiveness in detecting data tampering attempts and identifying rogue UAVs.

In the article by Yang et al. (2022) the security concerns and solutions for the Internet of Things are thoroughly reviewed, along with the security needs specific to the Internet of Things and the most recent developments in IoD security research. A variety of significant security technologies are examined in this analysis, with a focus on authentication methods and blockchain-based systems. The researchers outline the difficulties that existing approaches confront and suggest future IoD security research options based on a thorough review. This study reviews security vulnerabilities in the IoD discusses solutions already in place, and analyses the difficulties that IoD security faces. Although there are other defences and fixes, this research focuses on two key strategies: authentication and blockchain-based methods.

Maikol et al. (2021) suggest a brand-new authentication method for mobile users of cloud computing. The suggested remedy uses a key agreement mechanism with two layers of protection. The impersonation attack and MITM can be reduced, according to a thorough review of the current authentication technique and the suggested scheme. As it offers mutual authentication between sender and recipient, it helps to lower the danger of impersonation attacks. The likelihood of MITM will be reduced since the domain parameter used to generate the digital signature is chosen at random. The suggested remedy will entice more studies into cryptography-based two-layer security by researchers. The investigation demonstrates that these techniques would significantly improve and reinforce the medical system's data protection security.

3 Taxonomy

In this taxonomy, some things will be expressed in the awareness of the use of UAVs that are a weakness to the country's cyber security that refers to attacks and also techniques to repel from attacks:

3.1 Cyber Attack

A statement, in an article by Khoei et al. (2022) is a fraudulent attack through the GPS signal that can direct the UAV to lose control of the owner who will be disturbed by hackers who may once intend to steal the UAV from its original owner. According to Yang et al. (2022), the effort of hackers who want to hack specific organizations such as the military through IoD is very worrying when they can penetrate cyberspace through UAVs that are being done by the army. Similarly, Alrefaei et al. (2022) state that the hacker's act of jamming and spoofing is through the communication network of the UAV control device, and the hacker will penetrate the database in an organization. According to Pan et al. (2022), the hacker will turn off the cellular network which is the cellular service installed on the UAV itself as soon as the hacker can penetrate the network into the user's device that currently has a line with the UAV's cellular network. In addition, Abhishek et al. (2022) state that hackers will access data through UAVs in cyber data space, and it is very dangerous if hackers successfully enter this cyber data space.

3.2 Techniques Used to Mitigate Attacks

There are several methods and techniques to reduce attacks from hackers, namely, through the Classification Group Tree method and also the Regression technique that can detect the actions of hackers who want to hack through the UAV communication network (Khoei et al., 2022). On the other hand, Yang et al. (2022) suggest improving IoD techniques on UAVs by applying authentication techniques and block-powered schemes to avoid hacker attacks. According to Asghar Khan et al. (2022), a method of increasing the application of the authentication scheme is hyperelliptic curve cryptography (HECC), a technique aimed at digital signatures in preserving the privacy of the UAV user itself. Another technique is applying Blockchain Technology to UAVs (Tan et al., 2022) by storing UAV verification information at a low cost to industries and organizations that use these UAVs. Qiu et al. (2020) suggest applying blockchain on UAVs by increasing the chain spectrum on cellular networks installed on UAVs. The spectrum-sharing technique on UAVs stated in the article by Li et al. (2020) is designed to combat the eavesdropping of system secrecy and to further optimise the trajectory in further increasing the rate of secrecy with benchmarks. The method in the article by Na et al. (2022) further optimizes the trajectory in UAV communication that provides Internet of Things (IoT) resources to the community whose mobility has been installed on the UAV and with the results of the researcher's study of this article, it further increases the confidentiality of the IoT user's information itself.

4 Research Trends

The awareness of UAV users is to provide an understanding of using UAVs today, as stated in the article by Durfey and Sajal (2022), this UAV is a machine that can change the world today towards danger in putting an individual at risk involving the country. This article has researched the issue of cyber threats with the efforts of researchers so that the users of this UAV are safe from any cyber threats. Abhishek et al. (2022) stressed that the lack of integrity of data and information in the country should be curbed so that it does not leak to irresponsible parties, even though with the current technology, the country's cyber security should be tightened against any threat. While Lu et al. (2022) emphasized that the repeated algorithm is safe if it is applied to the use of UAVs, and this shows that this should be applied in the awareness course of the use of UAVs nowadays to be better understood.

Sun et al. (2022), noted that network collaboration is more secure in the use of this UAV because it has the characteristics of secure and energy-efficient communication multi-objective optimization problem (SECMOP) which can guarantee the safety of the community and the country. According to Ferrao et al. (2020), to increase the productivity and economy of the country, there are increasing market demands for UAVs because they greatly facilitate business for industries and organizations that practice the use of UAVs in addition to improving the characteristics of safety features for UAV users from time to time the original sentence is too long and confusing. Therefore, the awareness of the use of UAVs should be evaluated for the weaknesses and also the ability of these UAVs to be used in the future because the safety of the community and the country should be emphasized so that it is guaranteed and safe to be used in various sectors in the country today Chaari et al. (2020).

5 Challenges

In the challenge of giving awareness to UAV users, this should be studied and researched first before providing exposure to those who use this UAV tool so that its use is clear. Therefore, based on the article by Ying et al. (2019) safety involving air traffic may occur because it depends on the Automatic Dependent Surveillance-Broadcast (ADS-B) system used by the aviation department during monitoring by the International Civil Aviation Organization (ICAO) which points to measure a movement in space. Likewise, as stated in the article by Romesburg et al. (2021) the use of UAVs exploring the space path area in addition to the existence of Software-Defined Radio (SDR) because it applies a game system such as a UAV and also a penetration test for the radio system for the aviation department today, this is important to know in the challenge of widespread use of UAVs the meaning in this sentence is not clear. In addition to that, according to Tiu and Zolkipli (2021), a significant challenge is ransomware attacks which are no stranger nowadays because they are an alternative for hackers to carry out cyber-attacks.

Breaking down the cyber threat in the article by Durfey and Sajal (2022) it is a challenge to cyber security today. Moreover, it is widely used in various industries and also organizations to facilitate their work, the national defence department in cooperation with the authorities has taken the initiative in terms of misuse of this UAV tool. At the same time according to Wang et al. (2020) the most critical challenge is interference with CPS, especially with the data and information available in the country, the invasion can happen at any time without notification in detecting the country's cyber threat. We must look at this from all aspects so that the national communication network is always safe from any national cyber security intruding.

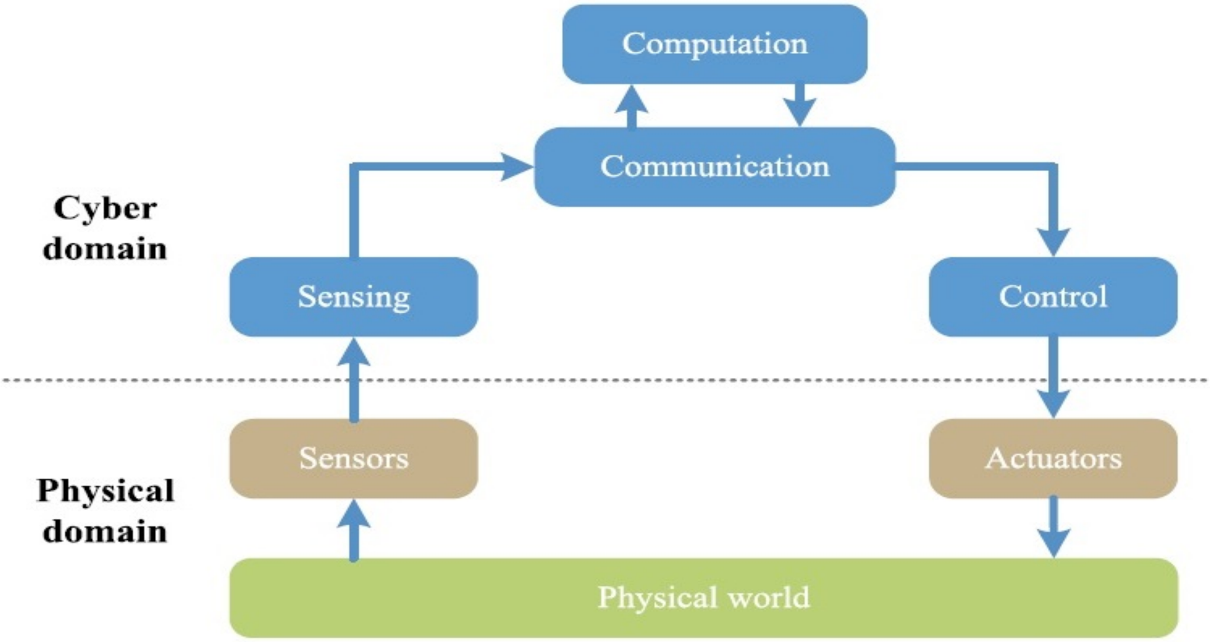


Figure 2: Cyber-physical system (CPS) diagram

Wang et al. (2020) discussed the integration of embedded systems on UAVs that allow them to be integrated with cyber processes into the physical UAV itself. Therefore, UAV is a Cyber-Physical System (CPS) which has three components which are cell level, system level, and system level in addition it is combined with CPS components as shown in figure 2 which is clear in dealing with any threat cyber-physical.

6 Future Direction

In the future direction, we can observe the widespread use of UAVs due to the many market requests, especially because they have the latest technological features to facilitate all work or affairs from various industries and organizations. According to Li et al. (2021), the production of UAV machinery needs to provide features that have been studied by researchers such as Bispectrum Siamese (BISSIAM) because these features will better guarantee security in applying network coding on UAV devices so that it is not misused in the future. Heo et al. (2022) considered the existence of UAVs as a contributor to the IoT today by establishing a block verification network with network coding widely which can guarantee any threat to UAV user misconduct. While Ma et al. (2022) stressed that this UAV has been promoted as a tool for providing data replacement services, content caching and also the implementation of computing tasks through Edge Computing Devices (ECD). With the existence of ECD, it focuses on algorithms for computing resources optimally in performing tasks, therefore, various workload tasks can be effectively overcome if applied with the characteristics stated by the researcher.

According to Al-Khafaji and Elwiya (2022), to further improve today's industrial technology such as Artificial Intelligence (AI) and Machine Learning (ML) is an important thing that must be further improved so that the country can progress with a sustainable economic position for the country and also the community. Abhishek et al. (2022) suggested that the spirit of increasing the integrity of UAV users should be fostered so that it is in line with the rules and laws in the use of UAVs to give more trust to the authorities. Some features must be present in the creation of UAVs in the future by applying Secure Internet-of-Drones (IoD) because applying Secure IoD is a low cost for the creation of UAVs in the future as stated by Pu et al. (2022). The most important thing for the future direction is to provide exposure and understanding to UAV users so that they are more alert to any cyber threat as stated by Abo Mosali et al. (2022). This is important in providing training or courses to those who apply its use in facilitating their tasks to industry and also organizations. In addition, Xing et al. (2022) emphasized that the features of UAVs can help in post-disaster situations, especially when there is a possibility of unexpected things happening such as no one has a cellular network due to the disaster and it is an alternative that will make it easier for the organization to carry out tasks such as monitoring. Lastly, deep learning methods, Blockchain and multifactor authentication methods can also be used and implemented to mitigate several communication attacks (Ahmad et al., 2020; Khan et al., 2021; Khan et al., 2022; Asim et al., 2022).

7 Conclusions

In conclusion, it is crucial for users in various industries nowadays to be exposed to and to be aware of using UAV tools. If necessary, users must have a license and have completed an official authority course before using UAVs. It is crucial to guarantee cyber security and strengthens the nation's defence against cyber threats by today's irresponsible actors. Therefore, the NGO side or the legislative body of the ministry of cyber security in Malaysia always emphasizes the responsibility of the superiors in an organization who need to play a critical role in cyber security and not just rely entirely on the information and technology (IT) department. At the same time, a strategic approach must be taken in addition to ensuring that their employees are aware of cyber security through workshops or courses implemented by the organization.

Therefore, the disclosure that provides ethics and integrity courses to UAV users is very important for the well-being of various parties especially when it can reduce the risk of cyber threats. In addition, the administration or human resources in an organization should always emphasize the Professional Development of Cyber Security in Malaysia, with the help of external agencies in cyber security which has now developed into a new platform to cultivate information security practitioners and knowledge sharing with leading industry experts and academics as well as fostering local and international cooperation to intensify the prevention of cyber security threats such as these UAVs from being misused by certain parties. At the same time fostering information security competence and specific training in Malaysia and is also the presenter of a line of competence courses from various programs and professional certifications aimed at meeting the needs of a fast and secure cyber landscape from unwanted threats. Therefore, the study of this article is expected to give awareness to UAV users to increase understanding as well as integrity and ethics in using UAV tools to deal with any threats from irresponsible parties in particular.

References

Abhishek, N. V., Aman, M. N., Lim, T. J., & Sikdar, B. (2022a). PIC: Preserving Data Integrity in UAV-Assisted Communication. IEEE INFOCOM 2022 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). https://doi.org/10.1109/infocomwkshps54753.2022.9798213

Abhishek, N. V., Aman, M. N., Lim, T. J., & Sikdar, B. (2022b). MaDe: Malicious Aerial Vehicle Detection using Generalized Likelihood Ratio Test. ICC 2022 - IEEE International Conference on Communications. https://doi.org/10.1109/icc45855.2022.9838465

Abo Mosali, N., Shamsudin, S. S., Alfandi, O., Omar, R., & Al-Fadhali, N. (2022). Twin Delayed Deep Deterministic Policy Gradient-Based Target Tracking for Unmanned Aerial Vehicle With Achievement Rewarding and Multistage Training. IEEE Access, 10, 23545–23559. https://doi.org/10.1109/access.2022.3154388

Ahmad, Z., Shahid Khan, A., Wai Shiang, C., Abdullah, J., & Ahmad, F. (2020). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. Transactions on Emerging Telecommunications Technologies, 32(1). https://doi.org/10.1002/ett.4150

Al-Khafaji, M., & Elwiya, L. (2022). ML/AI Empowered 5G and beyond Networks. 2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA). https://doi.org/10.1109/hora55278.2022.9799813

Alrefaei, F., Alzahrani, A., Song, H., & Alrefaei, S. (2022). A Survey on the Jamming and Spoofing attacks on the Unmanned Aerial Vehicle Networks. 2022 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS). https://doi.org/10.1109/iemtronics55184.2022.9795809

Alsamhi, S., Afghah, F., Sahal, R., Hawbani, A., Al-qaness, M. A., Lee, B., & Guizani, M. (2021). Green internet of things using UAVs in B5G networks: A review of applications and strategies. Ad Hoc Networks, 117, 102505. https://doi.org/10.1016/j.adhoc.2021.102505

Asghar Khan, M., Ullah, I., Alkhalifah, A., Ur Rehman, S., Ali Shah, J., Uddin, I., Alsharif, M. H., & Algarni, F. (2022). A Provable and Privacy-Preserving Authentication Scheme for UAV-Enabled Intelligent Transportation Systems. IEEE Transactions on Industrial Informatics, 18(5), 3416–3425. https://doi.org/10.1109/tii.2021.3101651

Asim, J., Khan, A. S., Saqib, R. M., Abdullah, J., Ahmad, Z., Honey, S., Afzal, S., Alqahtani, M. S., & Abbas, M. (2022). Blockchain-based Multifactor Authentication for Future 6G Cellular Networks: A Systematic Review. Applied Sciences, 12(7), 3551. https://doi.org/10.3390/app12073551

Chaari, L., Chahbani, S., & Rezgui, J. (2020). Vulnerabilities Assessment for Unmanned Aerial Vehicles Communication Systems. 2020 International Symposium on Networks, Computers and Communications (ISNCC). https://doi.org/10.1109/isncc49221.2020.9297293

Durfey, N., & Sajal, S. (2022). A Comprehensive Survey: Cybersecurity Challenges and Futures of Autonomous Drones. 2022 Intermountain Engineering, Technology and Computing (IETC). https://doi.org/10.1109/ietc54973.2022.9796881

Gromada, K. A., & Stecz, W. M. (2021). Designing a Reliable UAV Architecture Operating in a Real Environment. Applied Sciences, 12(1), 294. https://doi.org/10.3390/app12010294

Haider, M., Ahmed, I., & Rawat, D. B. (2022). Cyber Threats and Cybersecurity Reassessed in UAV-assisted Cyber Physical Systems. 2022 Thirteenth International Conference on Ubiquitous and Future Networks (ICUFN). https://doi.org/10.1109/icufn55119.2022.9829584

Heo, G., Chae, K., & Doh, I. (2022). Hierarchical Blockchain-Based Group and Group Key Management Scheme Exploiting Unmanned Aerial Vehicles for Urban Computing. IEEE Access, 10, 27990–28003. https://doi.org/10.1109/access.2022.3157753

Khan, A. S., Ahmad, Z., Abdullah, J., & Ahmad, F. (2021). A Spectrogram Image-Based Network Anomaly Detection System Using Deep Convolutional Neural Network. IEEE Access, 9, 87079–87093. https://doi.org/10.1109/access.2021.3088149

Khan, A. S., Balan, K., Javed, Y., Tarmizi, S., & Abdullah, J. (2019). Secure Trust-Based Blockchain Architecture to Prevent Attacks in VANET. Sensors, 19(22), 4954. https://doi.org/10.3390/s19224954

Khan, A. S., Javed, Y., Abdullah, J., & Zen, K. (2021). Trust-based lightweight security protocol for device to device multihop cellular communication (TLwS). Journal of Ambient Intelligence and Humanized Computing. https://doi.org/10.1007/s12652-021-02968-6

Khan, A. S., Javed, Y., Saqib, R. M., Ahmad, Z., Abdullah, J., Zen, K., Abbasi, I. A., & Khan, N. A. (2022). Lightweight Multifactor Authentication Scheme for NextGen Cellular Networks. IEEE Access, 10, 31273–31288. https://doi.org/10.1109/access.2022.3159686

Khoei, T. T., Gasimova, A., Ahajjam, M. A., Shamaileh, K. A., Devabhaktuni, V., & Kaabouch, N. (2022). A Comparative Analysis of Supervised and Unsupervised Models for Detecting GPS Spoofing Attack on UAVs. 2022 IEEE International Conference on Electro Information Technology (EIT). https://doi.org/10.1109/eit53891.2022.9813826

Li, T., Hong, Z., Cai, Q., Yu, L., Wen, Z., & Yang, R. (2021). BISSIAM: Bispectrum Siamese Network Based Contrastive Learning for UAV Anomaly Detection. IEEE Transactions on Knowledge and Data Engineering, 1–1. https://doi.org/10.1109/tkde.2021.3118727

Lu, X., Xiao, L., Niu, G., Ji, X., & Wang, Q. (2022). Safe Exploration in Wireless Security: A Safe Reinforcement Learning Algorithm With Hierarchical Structure. IEEE Transactions on Information Forensics and Security, 17, 732–743. https://doi.org/10.1109/tifs.2022.3149396

Ma, X., Su, Z., Xu, Q., & Ying, B. (2022). Edge Computing and UAV Swarm Cooperative Task Offloading in Vehicular Networks. 2022 International Wireless Communications and Mobile Computing (IWCMC). https://doi.org/10.1109/iwcmc55113.2022.9824275

Na, Z., Ji, C., Lin, B., & Zhang, N. (2022). Joint Optimization of Trajectory and Resource Allocation in Secure UAV Relaying Communications for Internet of Things. IEEE Internet of Things Journal, 9(17), 16284–16296. https://doi.org/10.1109/jiot.2022.3151105

Pan, X., Jin, Y., Wang, Z., & Li, F. (2022). A Pairing-Free Heterogeneous Signcryption Scheme for Unmanned Aerial Vehicles. IEEE Internet of Things Journal, 9(19), 19426–19437. https://doi.org/10.1109/jiot.2022.3167102

Pu, C., Wall, A., Ahmed, I., & Choo, K. K. R. (2022). SecureIoD: A Secure Data Collection and Storage Mechanism for Internet of Drones. 2022 23rd IEEE International Conference on Mobile Data Management (MDM). https://doi.org/10.1109/mdm55031.2022.00033

Qiu, J., Grace, D., Ding, G., Yao, J., & Wu, Q. (2020). Blockchain-Based Secure Spectrum Trading for Unmanned-Aerial-Vehicle-Assisted Cellular Networks: An Operator's Perspective. IEEE Internet of Things Journal, 7(1), 451–466. https://doi.org/10.1109/jiot.2019.2944213

Romesburg, H., Wang, J., Jiang, Y., Wang, H., & Song, H. (2021). Software Defined Radio based Security Analysis For Unmanned Aircraft Systems. 2021 IEEE International Performance, Computing, and Communications Conference (IPCCC). https://doi.org/10.1109/ipccc51483.2021.9679408

Maikol, S. O., Khan, A. S., Javed, Y., Bunsu, A. L., Petrus, C., George, H. & Jau, S. (2021). A Novel Authentication and Key Agreement Scheme for Countering MITM and Impersonation Attack in Medical Facilities. The International Journal of Integrated Engineering, 13(2), 127–135. https://doi.org/10.30880/ijie.2021.13.02.015

Sun, G., Li, J., Wang, A., Wu, Q., Sun, Z., & Liu, Y. (2022). Secure and Energy-Efficient UAV Relay Communications Exploiting Collaborative Beamforming. IEEE Transactions on Communications, 70(8), 5401–5416. https://doi.org/10.1109/tcomm.2022.3184160

Tan, Y., Wang, J., Liu, J., & Kato, N. (2022). Blockchain-Assisted Distributed and Lightweight Authentication Service for Industrial Unmanned Aerial Vehicles. IEEE Internet of Things Journal, 9(18), 16928–16940. https://doi.org/10.1109/jiot.2022.3142251

Tiu, Y. L., & Zolkipli, M. F. (2021). Study on Prevention and Solution of Ransomware Attack. Journal of IT in Asia, 9(1), 133–139. https://doi.org/10.33736/jita.3402.2021

Tomaszewski, L., Kołakowski, R., Dybiec, P., & Kukliński, S. (2022). Mobile Networks' Support for Large-Scale UAV Services. Energies, 15(14), 4974. https://doi.org/10.3390/en15144974

Wang, H., Zhao, H., Zhang, J., Ma, D., Li, J., & Wei, J. (2020). Survey on Unmanned Aerial Vehicle Networks: A Cyber Physical System Perspective. IEEE Communications Surveys &Amp; Tutorials, 22(2), 1027–1070. https://doi.org/10.1109/comst.2019.2962207

Wu, J., Guo, J., & Lv, Z. (2022). Deep Learning Driven Security in Digital Twins of Drone Network. ICC 2022 - IEEE International Conference on Communications. https://doi.org/10.1109/icc45855.2022.9838734

Xing, R., Su, Z., Luan, T. H., Xu, Q., Wang, Y., & Li, R. (2022). UAVs-Aided Delay-Tolerant Blockchain Secure Offline Transactions in Post-Disaster Vehicular Networks. IEEE Transactions on Vehicular Technology, 71(11), 12030–12043. https://doi.org/10.1109/tvt.2022.3184965

Yang, W., Wang, S., Yin, X., Wang, X., & Hu, J. (2022). A Review on Security Issues and Solutions of the Internet of Drones. IEEE Open Journal of the Computer Society, 3, 96–110. https://doi.org/10.1109/ojcs.2022.3183003

Yin, Z., Jia, M., Cheng, N., Wang, W., Lyu, F., Guo, Q., & Shen, X. (2022). UAV-Assisted Physical Layer Security in Multi-Beam Satellite-Enabled Vehicle Communications. IEEE Transactions on Intelligent Transportation Systems, 23(3), 2739–2751. https://doi.org/10.1109/tits.2021.3090017

Ying, X., Mazer, J., Bernieri, G., Conti, M., Bushnell, L., & Poovendran, R. (2019). Detecting ADS-B Spoofing Attacks Using Deep Neural Networks. 2019 IEEE Conference on Communications and Network Security (CNS). https://doi.org/10.1109/cns.2019.8802732

Recapitulation of Survey on Taxonomy: Security Unmanned Aerial Vehicles Networks

[1]Veronica Sima Anak Kilat,[2*]Adnan Shahid Khan, [3]Eunice James and [4]Nayeem Ahmad Khan

[1,2,3]Faculty of Computer Science and Information Technology, 94300 Kota Samarahan, Sarawak, Malaysia
[4]Faculty of Computer Science and Information Technology, AlBaha University, AlBaha, Saudi Arabia

email: [1]22030072@siswa.unimas.my, [2*]skadnan@unimas.my, [3]21030614@siswa.unimas.my, [4]nayeem@bu.edu.sa

*Corresponding author

Received: 04 September 2022 | Accepted: 11 April 2023 | Early access: 26 April 2023

Abstract - *The operation of unmanned aerial vehicles (UAVs) presents various challenges for radio spectrum management. It is crucial to ensure safety, effective spectrum use, and compatibility with existing wireless networks. However, the dynamic nature of UAV networks requires adaptive spectrum decisions and resilient schemes that can provide reliable services. Current spectrum schemes may have limitations when used in UAV networks. Nevertheless, the integration of communication technology, computation power, and control modules in UAV networks can construct a comprehensive sequence of data detecting, intelligence transferring, deliberation, and final implementation, which facilitates cyber processes in physical devices. This integration turns the UAV network into a cyber-physical system (CPS). The internet of everything (IoE) is the concept of an all-encompassing network connecting everything. It is facing significant obstacles, such as limited broadband service and shortages in existing network technology. UAVs have recently gained attention due to their mobility, affordability, and versatility. They have the potential to circumvent the challenges faced by IoE. This paper aims to provide an overview of UAVs from a different perspective, highlighting the challenges they present and discussing future research directions to ensure a proper plan for the future. With the proliferation of UAVs, it is essential to address issues related to their safe operation, efficient use of spectrum, and compatibility with existing networks. Moreover, research should focus on developing resilient schemes that can deliver smooth and reliable services in UAV networks. In conclusion, the operation of UAVs poses several challenges for radio spectrum management, but they also offer opportunities for innovation and development. The integration of communication technology, computation power, and control modules in UAV networks turns them into cyber-physical systems with the potential to overcome the challenges faced by IoE. Further research is necessary to ensure safe and efficient operation, and to explore the possibilities that UAVs offer for the future.*

Keywords: Unmanned Aerial Vehicle (UAV), Security, IoE, Cyber Security.

1 Introduction

Unmanned aerial vehicles (UAVs), often known as drones, are becoming increasingly essential in a variety of fields, including both the military and the civilian spheres. These qualities, along with their relatively low cost and ease of deployment, contribute to the UAVs' growing prominence (Fotohi, 2020). When it comes to military applications, UAVs are anticipated to become an essential component of the future frontlines. Not only are they able to proactively capture a variety of information on a vast scale in terms of both time and location, but they may also benefit other unmanned and manned combat platforms in completing potentially hazardous operations. UAVs' flight can be remotely piloted by a human, similar to remotely piloted aircraft (RPA), or they can have varying ranges of autonomy, such as autopilot help, up to fully autonomous aircraft that don't allow for human intervention. Nowadays, the majority of UAVs have the ability to conduct both attack and surveillance missions. UAVs are also being utilised more frequently for non-commercial purposes, like putting out fires. UAVs are often used in missions that are very "boring, dirty, or dangerous" for a guided aircraft.

In addition to military applications, UAVs are being used in a wide range of civilian applications. They are being used for surveying and mapping, monitoring wildlife and environmental conditions, inspecting infrastructure such as bridges and power lines, conducting search and rescue operations, and delivering goods and services. In the agricultural sector, UAVs are being used to monitor crop health, track weather patterns, and optimize irrigation and fertilizer use. The construction industry is using UAVs for site surveying, tracking construction progress, and inspecting structures (Mohammad et al., 2023).

UAVs are also being used for entertainment purposes, such as in aerial photography and videography for film and television production. They are also used in sports broadcasting, providing unique and exciting camera angles and perspectives that were previously unavailable.

One of the most significant benefits of UAVs is their ability to access hard-to-reach areas, such as disaster zones or remote wilderness areas. UAVs can provide real-time information to emergency responders, allowing them to make more informed decisions and save lives. In the field of wildlife conservation, UAVs are being used to monitor endangered species and to identify and prevent illegal poaching.

As UAV technology continues to advance, there are increasing concerns about privacy and security. Regulations around the use of UAVs are being developed to address these concerns, with restrictions on where and when they can be flown and what they can be used for. Despite these concerns, the growing versatility and affordability of UAVs are driving their increased use in a wide range of applications.

This survey article will discuss conceptually related works, taxonomy from the perspectives of attacks, and techniques used to mitigate the attacks. Furthermore, the end of this article will elaborate more on research trends and challenges faced, and discuss the future direction of UAVs. A few figures and tables can be referenced based on related works from various authors. This paper includes the abstract, introduction, related summary, taxonomy, research trends, challenges, future directions, conclusion, acknowledgement, and references.

2 Related Works

2.1 Survey on Networks of Unmanned Aerial Vehicles: Considerations from a Cyber-Physical Perspective

According to Wang (2019) discussion on dual cyber-physical systems (CPS), unmanned aerial vehicle (UAV) networks are gaining significant interest due to the benefits they offer in expanding human behavior without direct human involvement. Wang (2019) suggests that embedding UAVs into the CPS platform or creating UAV networks from the perspective of CPS could enhance their efficiency in performing various complex tasks. The study aims to conduct a comprehensive analysis of the CPS in relation to UAV networks.

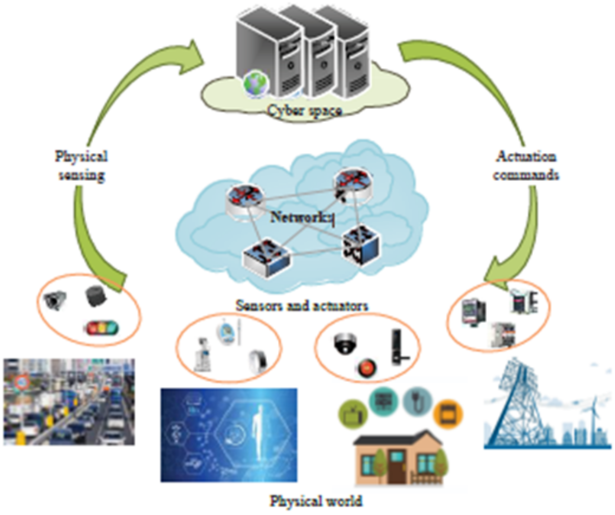


Figure 1: A conventional CPS framework

The author (Wang, 2019) acknowledges that both CPS and UAV networks are interdisciplinary, challenging, but exciting fields. The requirements, difficulties, and technology involved are numerous and continually evolving. This brief overview aims to provide a concise primer for newcomers and a cutting-edge CPS perspective to help researchers address the interdisciplinary issues. The author is confident that encouraging collaboration between CPS and UAV networks will strengthen both fields and improve our quality of life.

The National Aeronautics and Space Administration (NASA) was the first organization to recommend cyber-physical systems (CPS) for use in space research with unmanned aircraft. Since then, CPS has been applied to combat situations to reduce losses, where soldiers can remain in a staging area and operate weapons remotely, without physically being present on the battlefield. CPS has now been widely implemented in many society-critical areas as part of the "Industry 4.0" movement. This includes areas such as transportation, energy, healthcare, and manufacturing.

2.2 Opportunities and challenges presented by unmanned aerial vehicles in the context of the Internet of Everything

Research by Liu et al. (2020) aims to enhance the capabilities of the Internet of Everything (IoE) by utilizing unmanned aerial vehicles (UAVs) to improve its comprehensive understanding, flexible intelligence, and more varied applications. The implementation of IoE faces several obstacles related to coverage, battery, processing, and security concerns to meet the three IoE expectations of scalability, intelligence, and diversity. UAVs, with their high mobility and adaptable deployment, have the potential to assist IoE in overcoming these difficulties. In this context, Liu et al. (2020) have conducted a thorough analysis of the possibilities and fixes for UAVs in IoE, with two key components of the review being the UAS design and the analysis of UAV communication networks. The authors have investigated a variety of UAV applications in IoE, including ubiquitous connections, on-demand aerial intelligence, self-maintenance, power supply, sensor recycling, and more. Additionally, the authors have discussed current problems and Ue-IoE directions. Overall, the authors have thoroughly analyzed the advantages and disadvantages of deploying UAVs in IoE. For future investigations on Ue-IoE, this survey can serve as a study direction.

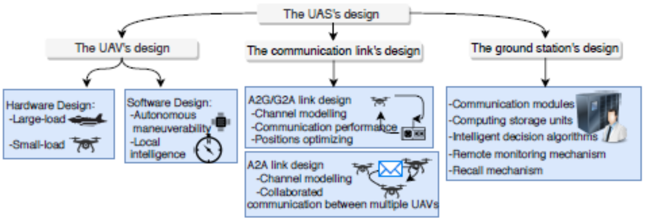


Figure 2: A system's unmanned aircraft design methodology (UAS)

2.3 Autonomous Spectrum Management for UAV Disaster Relief

In their research, Shamsoshoara et al. (2020) addressed the issue of spectrum scarcity in UAV networks during crucial missions, such as search and rescue operations, monitoring disasters, and wildfires. These missions require high-speed data transfers, including real-time streaming of speech, pictures, and video, and the spectrum allocated to the UAV network may not be sufficient to provide the required Quality of Service (QoS). Therefore, the researchers proposed a model for sharing the spectrum, in which one UAV serves as a relay, which transmits data to a grounded network in exchange for the necessary spectrum. Other UAVs can then use this spectrum to communicate the sensed data. The proposed approach was compared to other random distributions and assignments. The researchers also suggested offline learning to create a predetermined Q-table for larger grid-size planes, taking into account the exact location of the grid's aircraft for unsafe and dangerous areas, which saves time. Afterward, the UAVs can automatically move to the best place based on the Q-table in a completely greedy manner. The proposed approach can provide the necessary spare spectrum to the UAV network during crucial missions, improving the network's performance and maintaining QoS. The researchers' proposed approach can be useful in various applications, including monitoring disasters, search and rescue operations, and wildfires.

2.4 Framework for a Mutual Authentication Protocol that is Both Safe and Effective for Use with Unmanned Aerial Vehicles

Bansal and Sikdar’s (2021) study focuses on the security and privacy concerns of UAV-based applications, such as man-in-the-middle, replay, and physical attacks. The authors suggest using a lightweight mutual authentication method, which utilizes Physically Unclonable Functions (PUF) devices, to counter these threats and provide network and communication security. The significance of this solution lies in the protection it provides against threats like man-in-the-middle, replay, and physical attacks, as the communications between base stations and UAVs are already encrypted. The attackers' primary motive for targeting UAVs is to hijack them for personal interests. The UAV applications discussed in the study include medical surveillance, traffic monitoring, military operations, and package delivery. To assess the feasibility of this solution for future proposals and research, one could consider adopting and applying the technology in any of the aforementioned fields, such as medical surveillance, military operations, or package delivery.

Figure 3: one example of a commonly used Drone or UAV

2.5 Efficient Certificateless Signcryption for UAV Cluster Network

In their article, Da et al. (2021) focus on the security risks associated with wireless channels used for UAV-to-UAV and UAV-to-CS interactions in open environments, such as eavesdropping, SQL intrusions, and denial-of-service attacks. The authors suggest that limited computational and storage capabilities of single UAVs make it difficult for them to transmit large amounts of data over long distances. To overcome these limitations and to address security and privacy concerns in UAV cluster network applications, the authors propose the use of a Certificateless Aggregate Signcryption (CL-ASC) system that ensures data privacy and the reliability of data sources. This approach is particularly important for UAV applications in both military and civilian settings, including freight transportation, security patrols, regional surveillance, disaster rescue, and catastrophe monitoring. The authors suggest that future research should focus on developing and implementing CL-ASC systems as the best solution for securing UAV cluster network applications.

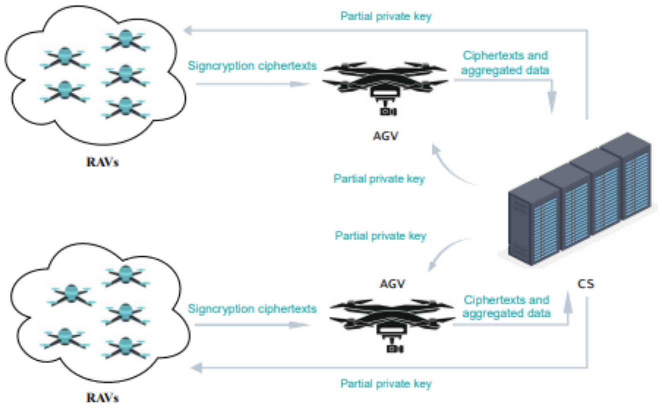


Figure 4: UAV cluster network data-collection model

2.6 Threats, opportunities, and research ahead for secure UAV swarm mesh networks

A study conducted by Lopez et al. (2021) aimed to address the security and reliability issues of Wireless Mesh Networks (WMNs) for UAV swarm networking. The authors highlighted the vulnerabilities of WMNs and suggested a security-focused UAV mesh communication architecture to provide a solution to the challenges encountered in using mesh technology in the context of UAV swarms. The significance of implementing this solution is to overcome the weaknesses in the communication stack and to address the major obstacles to using mesh technology in UAV swarms. The primary goal of attackers targeting UAV swarms is to disrupt or manage communication within the network as mesh UAV communications have vulnerabilities that can be easily exploited at every level of the network. The UAV swarm's application discussed in the article aims to provide an ad hoc networking architecture for various tasks, from simple ones like geographic mapping, to complex missions like military operations or natural disaster response. Future recommendations include the implementation of the proposed architecture to address the vulnerabilities in UAV swarm communication.

Table 1: A breakdown of the hazards and openings facing mesh swarm connection for unmanned aerial vehicles

Layer	Threat/Vulnerability	Exploits	Defence/Opportunity
Physical	Passive Eavesdropping RF Jamming	Broadcast Nature of Wireless Channels Wireless contention	Strong Encryption Avoid Interference Zones
Link	Spoofing Frame Modification	Intentional Collision MAC Spoofing	Intrusion Detection Systems (IDS) Encryption
Network	Routing Forwarding Data Forwarding	Selfish Attacks Collusion Attacks	Intrusion Detection System (IDS) Firewall
Transport	Packet Corruption Protocol Weakness	Denial of Service (DoS) Session Hijacking	Intrusion Detection Systems (IDS) Transport Layer Security (TLS)
Application	ROS2 Bugs Open Protocols	Malware Injection/Modification	Authentication Encryption

2.7 A hypothetical method for self-adaptive UAV routing to reduce the risk of forest fires

In a study by Kilic and Ozkan (2019), a paradigm is presented for reducing the risk of forest fires using self-adaptive, autonomous UAVs. The authors use the memoryless exponential distribution to calculate the probability of forest fires. Due to the stochastic and dynamic nature of the problem and the mathematical complexity of the scheduling technique, a simulation analysis was performed.

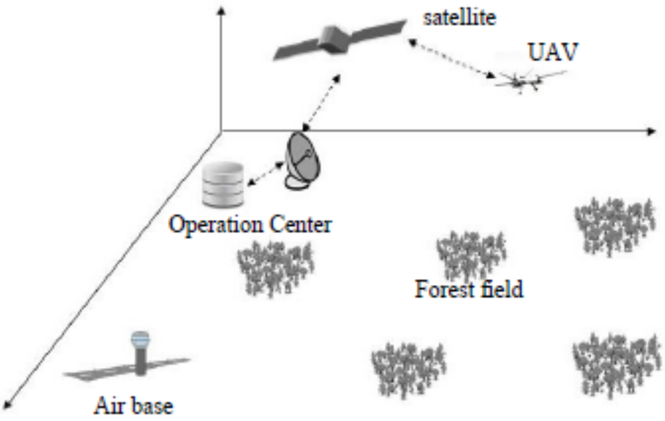


Figure 5: The proposed model's concept map (taken from Kilic & Ozkan, 2019, pp 1-12)

The main contribution of the proposed model is the assessment of the impact of inaccessible time and fire likelihood in candidate fields during UAV routing for forest fire detection. The suggested dispatching rule would make a significant contribution due to its memoryless nature if time delays for fire events in a field follow an exponential distribution.

The proposed conceptual model could also be seen as an earlier investigation for a data integration model. By using the proposed dispatching rule, a model that combines a repository of historical data, wireless sensors in fields, and satellite communications to collect and draw conclusions from data about the likelihood of fires in fields could lead to UAVs that can navigate on their own.

2.8 A study on the advancements, standardisation, and applications of UAVs in various sectors.

A study conducted by Mohsan et al. (2022) focuses on the drone industry, which has generated significant interest as a case study for the convergence of production, service, and delivery in various emerging sectors. UAVs offer several advantages, such as longer flight durations, higher cargo capacities, quick mobility, and access to remote and disaster-prone areas. The authors of this study examined recent UAV research developments in both the commercial and academic sectors. They provided a comprehensive analysis of UAV types, classifications, swarms, and charging methods, as well as the standardisation of UAVs. The authors demonstrated a growing interest in utilising UAV technology among government agencies, commercial organisations, and researchers. The study briefly discussed UAV characteristics such as flying time, acceleration, distance, altitudes, and capacity. Furthermore, the research offers a comprehensive analysis of UAV applications, challenges, and security issues. Specifically, the study explored the role of UAVs in IoT networks and 5G innovations. The authors concluded their analysis by identifying the research gap in UAV technology and outlining potential future research directions. The research offers a valuable insight into the current state of UAV technology and highlights its potential applications in various sectors. The study provides a foundation for further research to expand the capabilities of UAVs and increase their adoption in commercial and government applications.

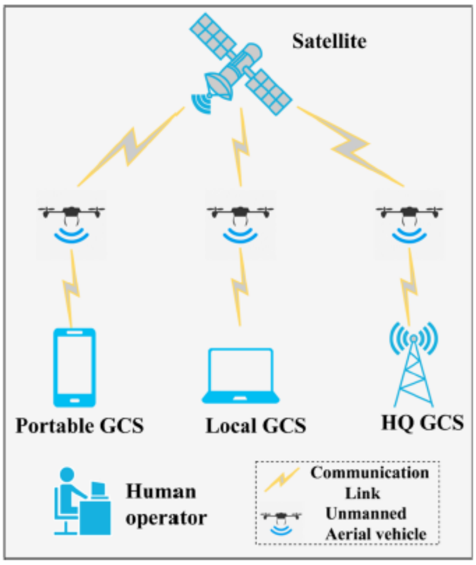


Figure 6: Architecture of UAV system

2.9 Computation offloading using heterogeneous and collective intelligence in aerial edge networks

A recent study by Su et al. (2022) focused on unloading tasks with the help of unmanned aerial vehicles (UAVs) on aerial edge networks (AEN). The authors propose a strategy that optimizes the offloading job options and the positioning of UAVs while considering the constraints of latency and overall UAV energy consumption. The objective of this study is to minimize the overall energy usage of all user equipments (UEs). This is a highly nonlinear problem that involves the coupling of several optimization variables. To overcome this challenge, the authors used reformulation linearization technology to convert the original optimization problem into a linear convex optimization problem. Then, they suggested using the alternating direction method of multipliers (ADMM) technique to arrive at the approximate optimal solution. The suggested ADMM method successfully reduces the total amount of energy consumed by UEs while maintaining their uninterrupted functioning, as per the numerical data. The authors also developed an ADMM-based incremental alternating strategy and inserted auxiliary variables into the equation to transform the problem into a linear form once again. Numerical data revealed that the suggested offloading technique has the potential to substantially reduce the total energy usage in comparison to the benchmarks. In the future, the research will investigate the dynamic distribution of processing capacity in collaborative computing networks that include many UAVs.

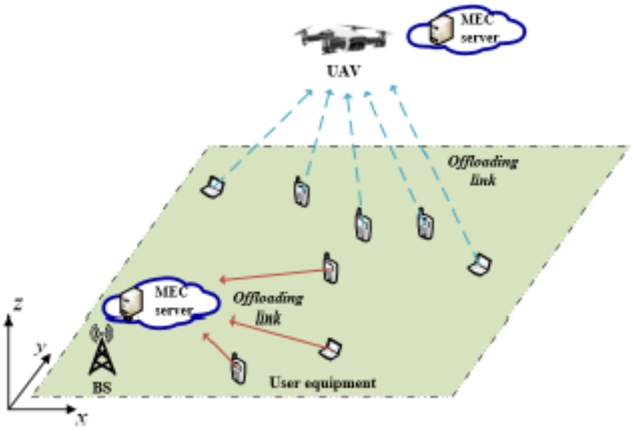


Figure 7: Model of MEC network aided by UAVs

2.10 Autonomous vehicle-based upcoming security and surveillance systems

Ayub (2018) conducted a study on the development and design of Unmanned Ground Vehicles (UGV) and Unmanned Aerial Vehicles (UAV) for safeguarding highly sensitive areas against incursion or any suspicious activity. The study described the development of a self-governing navigation algorithm and repetitive path following for UGV, which was effectively tested for both indoor and outdoor sites. The study also proposed a new approach for geolocation and autonomous flight of UAVs, which uses the Haver-Sine formula for complex geometry calculations and a reliable sensor network to adapt to UAV flight behavior. Ayub (2018) stated that an intelligent security and surveillance system was provided in the study, where the developed UGV can follow an user-selected path independently and broadcast live video feed from the site. Additionally, a fully autonomous flight control algorithm based on the straight earth approximation and Haversian Formula was proposed to utilize the surveillance and monitoring potential of UAVs. For autonomous flight, RC control, which has a limited operating range, is bypassed. To translate the 6-channel RC controlled signals for THROTTLE, YAW, ROLL, and PITCH, the study established the following information: 54.3% frequency, 5.55% to 10.88% duty cycle, and 784 mV to 1.08 vrms range. The MyRio then generates these signals and sends them to the remote control, whose operations are managed at the ground station. To ensure end-to-end authentication, the study proposed other solutions that can also be deployed (Khan et al., 2015, 2017, 2021, Maikol et al., 2020).

Designing a security and monitoring system for high-risk areas requires an innovative approach that integrates the functionalities of UGVs and UAVs, especially as centralised command and control systems become more prevalent (Dildar et al., 2017; Ahmad et al., 2020; Alqarni et al., 2022; Alshehri et al., 2023; Khan et al., 2023;). The study by Ayub (2018) offers a novel approach that can improve the capabilities of UGVs and UAVs for security and surveillance purposes. Further research can explore the potential of integrating these vehicles with other technologies to enhance security measures in high-risk areas.

3 Taxonomy

3.1 Attacks

1. Replay Attacks: In this attack, an attacker intercepts data packets between the sender and receiver, stores them, and later uses them to communicate with the receiver. This attack can occur between the server and the UAV or between the UAV and the BSH.
2. Unauthorized Data Tampering: This attack involves the unauthorized modification of data, which compromises the reliability of the information stored. Both insiders and outsiders can be the attacker in this scenario, and the attack can result in the data being changed if the USB or server is compromised.
3. Unlawful Access: This attack involves the installation of malware on a system to gain unauthorized access to critical data. The attacker may steal data covertly or cause damage to the system.

4. Man-in-the-Middle Attacks: In this type of attack, an external attacker intercepts communication between the server and UAV or between the UAV and the BSH. The attacker can gather sensitive data and modify it, compromising the system's security.

In summary, the proposed autonomous unmanned vehicle health monitoring system based on Blockchain by Raj (2021) faces various security threats such as replay attacks, unauthorized data tampering, unlawful access, and man-in-the-middle attacks. These attacks can compromise the integrity and confidentiality of the data stored in the system, and insiders and outsiders can be potential attackers. Hence, it is crucial to have effective security measures in place to mitigate these threats (Khan et al., 2019; Khan et al., 2021).

3.2 Techniques used to mitigate attacks

1. Replay Attack Protection Technique:
   Replay attacks can be detected through physical watermarking, which adds random noise to control inputs and looks for system reactions (Zhao & Smidts, 2020):
   a. A chi-squared test can be used with sensor measurements to determine a null hypothesis or alternative hypothesis (Zhao & Smidts, 2020).
   b. Random noise can be optimized to maximize replay attack detection while minimizing control performance loss (Khan et al., 2020).
   c. A zero-sum, finite-horizon stochastic game can be used to find the best strategy for alternating between ideal and undesirable controllers (Iqbal et al., 2011).
2. Unauthorized Data Tampering Protection Technique:
   a. A Wireless Channels Radio Checking Subsystem (WCRCS) can be incorporated into the design of the IoD monitoring system to provide cyber control and protection against RF vulnerabilities (Torianyk, 2021).
   b. WCRCS control capabilities can be augmented with transmitting and receiving protection, IoD restructuring, and other activities to form an RFV protection system (RFVPS) (Torianyk, 2021).
   c. RFVPS can be integrated into an overall cybersecurity assurance system (CSAS) to reduce the risk of vulnerabilities on RFVs and cyber failures caused by attacks (Torianyk, 2021).
3. Illegal UAV Access Protection Technique:
   a. Anti-UAV techniques can be employed to prevent attacks from UAVs, including intercepting communication channels and disrupting flight patterns (Chamola, 2021).
   b. Case studies of intentional UAV attacks can help understand the harm caused and how it can be prevented (Chamola, 2021).
   c. Techniques for monitoring and attacking UAVs, such as disrupting communication networks and removing autopilot software, can be employed (Chamola, 2021).
4. Man in the Middle UAV Attack Protection Technique:
   a. DroneSig uses a Duffing map to create a digital signature for encoding and decoding binary data without using popular cryptographic techniques like DES or AES (Li & Pu, 2020).
   b. DroneSig includes byte substitution, matrix transformation, and random shuffle operations (Li & Pu, 2020).

4 Challenges associated with drones

Drones present several significant challenges, one of which is their potential to violate privacy by capturing images and videos without consent. This issue is especially concerning in residential neighborhoods and public places. Additionally, drones can be used for illegal activities like drug trafficking and smuggling, which pose significant security concerns. Another challenge is the vulnerability of drones to hacking, as wireless communication systems can be intercepted and manipulated by hackers. Hacked drones can then be controlled by someone else, posing threats to public safety. Physical attacks like shooting down drones, using nets, or jamming their communication systems can also compromise drone security. However, there are various ways to defend against drone attacks. Anti-drone technology, including jamming devices and detection systems, can help authorities identify and respond to potential threats. Physical defenses like netting systems or trained birds of prey can capture drones, while defensive mechanisms like countermeasures and emergency landing systems can deflect and mitigate attacks. Governments can also impose regulations on the use of drones, such as requiring registration and licensing for their operation. Overall, effective defense against potential drone attacks requires a combination of technological and legislative measures.

5 Research trends, challenges and future direction

Research trends in Malaysia are influenced by security challenges arising from the use of drones or unmanned aerial vehicles (UAVs) that pose a threat to public safety and national security. The lack of regulation and monitoring of drone sales in the market has contributed to this problem (Abdullah et al., 2021). Although regulations have been introduced under the Malaysian Civil Aviation Regulations 2016 (MCAR 2016), they only apply to airport areas, making it difficult to ensure compliance for every drone owned by individuals. The sale of affordable drones in Malaysia has made it challenging for authorities to control and enforce regulations (Ismail et al., 2020).

Apart from security challenges, the Internet of Everything (IoE) faces several obstacles, including coverage, battery, computing, and security constraints (Lian et al., 2020). To overcome these challenges, efficient preventative measures need to be implemented. This includes constructing adaptable and recoverable networks to extend IoE coverage, creating environmentally friendly energy-supply systems to extend the lifecycle of IoE nodes, and coordinating the use of edge computing with local and cloud computing to make the most of available computing resources. Lastly, trustworthy security solutions need to be developed to safeguard data stored in pervasive IoE networks against intrusion attempts (Al-Fuqaha et al., 2015).

The use of drones with multiple layers presents several challenges that need to be addressed. According to Sekander et al. (2018), drones with multitiered capabilities have the potential to take control of cellular signals, especially during a catastrophe. However, the integration of drone networks into terrestrial networks can also bring potential benefits, such as unloading traffic and reducing the number of handovers for mobile users. To fully harness these benefits, the deployment of drone-aided cellular networks and air traffic control systems must first be addressed to avoid congestion in the future. Additionally, the confidentiality and safety of connected sensor devices in the Internet of Drones (IoD) must be given higher importance in the design of drone applications. The susceptibility of these devices to theft, malfunction, and misplacement poses significant risks that require mitigation strategies, such as controlling the electromagnetic field of carrier signals and employing risk reduction principles in court. Coordination and task scheduling also pose a challenge in the integration of cloud and edge computing for computationally expensive Internet of Things applications. Abdelmaboud (2021) suggests that external intelligent network applications require adequate centralised AI analysis and individual big data analysis to facilitate collaboration. Sequencing of computing jobs and evaluating the necessity of remote cloud migration require modifications to computer architecture and networking for optimal performance on a global scale.

Given these challenges, it is crucial to conduct a study on consumer behaviour and trends in drone use in Malaysia. This study can provide essential information to relevant agencies to find solutions to the raised issues. Specifically, the deployment of drone-aided cellular networks and air traffic control systems must be addressed to prevent congestion in the future. The confidentiality and safety of connected sensor devices in the IoD must also be given higher importance in the design of drone applications, and mitigation strategies such as controlling the electromagnetic field of carrier signals must be employed. Lastly, coordination and task scheduling pose a challenge in the integration of cloud and edge computing for computationally expensive Internet of Things (IoT) applications, requiring modifications to computer architecture and networking for optimal performance on a global scale.

In conclusion, the challenges presented by the integration of drones into terrestrial networks and the IoT require significant attention to harness their potential benefits. While addressing these challenges, it is important to consider the safety and confidentiality of connected sensor devices, as well as the coordination and scheduling of tasks. By conducting a study on consumer behaviour and trends in drone use, relevant agencies can develop effective solutions to these issues, leading to the safe and efficient deployment of drone networks in the future.

The next research plan involves the creation of a UAV swarm digital twin system. Professor Michael Grieves from the University of Michigan is credited with the concept of digital twins, which refers to virtual models that mimic the behaviour of real-world objects (Zhou, 2020). The digital twin system is designed to perceive data from the real-world UAV cluster and utilize it to make accurate predictions, estimates and observations about dynamic changes (Kar et al., 2022). With the development of this system, it is possible to understand complex commands, execute tasks autonomously and identify the best course of action in a given situation. Additionally, deep learning methods, blockchain and multifactor authentication techniques can be employed to counteract communication attacks (Kar et al., 2020; Zeeshan et al., 2021; Khan et al., 2021; Khan et al., 2022; Asim et al., 2022). It is anticipated that the proposed UAV swarm digital twin system will provide significant benefits in terms of improving task execution, operational efficiency and overall performance.

6 Conclusion

In conclusion, this survey article has provided an overview of unmanned aerial vehicles (UAV), also known as drones, and their potential to increase productivity in various industries. With the integration of embedded systems, communications technology, and control modules, the UAV network has the ability to establish a complete sequence of data perceiving, information transferring, deliberation, and final implementation, creating a cyber-physical system (CPS). Additionally, the concept of the internet of everything (IoE) has been discussed as an extension of the internet of things (IoT). This article has also presented a taxonomy of attacks and techniques to mitigate them, along with research trends, challenges, and future directions for the use of drones. Overall, this article has summarized related works and provided a comprehensive understanding of the current state of drones and their potential for the future.

References

Abdelmaboud, A. (2021). The Internet of Drones: Requirements, Taxonomy, Recent Advances, and Challenges of Research Trends. Sensors, 21(17), 5718.

Ahmad, Z., Khan, A. S., Cheah, W. S., Abdullah, J., & Ahmad, F. (2020). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. Transactions on Emerging Telecommunications Technologies, vol. 32 no.1, pp. e4150.

Alqarni, A. A., Alsharif, N., Khan, N. A., Georgieva, L., Pardade, E., & Alzahrani, M. Y. (2022). MNN-XSS: Modular neural network based approach for XSS attack detection. Computers, Materials and Continua, 70(2), 4075-4085.

Alshehri, A., Khan, N., Alowayr, A., & Alghamdi, M. Y. (2023). Cyberattack Detection Framework Using Machine Learning and User Behavior Analytics. Computer Systems Science and Engineering, 44(2), 1679-1689.

Asim, J., Khan, A. S., Saqib, R. M., Abdullah, J., Ahmad, Z., Honey, S., Afzal, S., Alqahtani, M. S., & Abbas, M. (2022). Blockchain-based Multifactor Authentication for Future 6G Cellular Networks. : A Systematic Review. Appl. Sci., 12, 3551.https:// doi.org/10.3390/app12073551.

Ayub, M. F., Ghawash, F., Shabbir, M. A., Kamran, M., & Butt, F. A. (2018). "Next Generation Security And Surveillance System Using Autonomous Vehicles,". Ubiquitous Positioning, Indoor Navigation and Location-Based Services (UPINLBS), pp. 1-5, doi: 10.110.

Bansal, G., & Sikdar, B. (2021). A Secure and Efficient Mutual Authentication Protocol Framework for Unmanned Aerial Vehicles. In 2021 IEEE Globecom Workshops (GC Wkshps). pp. 1-6.

Chamola, V. K. (2021). A comprehensive review of unmanned aerial vehicle attacks and neutralization techniques. Ad hoc networks, 111, 102324.

Da, L., Wang, Y., Ding, Y., Xiong, W., Wang, H., & Liang, H. (2021). "An Efficient Certificateless Signcryption Scheme for Secure Communication in UAV Cluster Network IEEE Intl Conf on Parallel & Distributed Processing with Applications, p 884-891.

Dildar, M. S., Khan, N., Abdullah, J., & Khan, A. S. (2017) "Effective way to defend the hypervisor attacks in cloud computing." In 2017 2nd International Conference on Anti-Cyber Crimes (ICACC), pp. 154-159. IEEE, 2017.

Fotohi, R. (2020). Securing of Unmanned Aerial Systems (UAS) against security threats using human immune system. Reliability Engineering & System Safety, 193, 106675.

Iqbal, A. M., Iqbal, S., Khan, A. S., & Senin, A. A. (2013). "A Novel Cost Efficient Evaluation Model for Assessing Research-Based Technology Transfer between University and Industry." Jurnal Teknologi 64(2).

Iqbal, A. M., Khan, A. S., Abdullah, J., Kulathuramaiyer, N., & Senin, A. A. (2021). Blended system thinking approach to strengthen the education and training in university-industry research collaboration. Technology Analysis & Strategic Management DOI: 10.1080/09537325.2021.1905790

Kar, H. A., & Rather, G. M. (2020). Multilayer Software Defined Networking Architecture for the Internet of Things. International Journal of Computing and Digital Systems, 9(4), 735-746.

Kar, H. A., & Rather, G. M. (2020, March). An analytical and simulation study of round trip transmission time of an edge based Internet of Things network. In 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA) (pp. 538-543). IEEE.

Khan, A.S., Ahmad, Z., Abdullah, J. & Ahmad, F. A. (2021). Spectrogram Image-Based Network Anomaly Detection System Using Deep Convolutional Neural Network. IEEE Access, 9, 87079–87093.

Khan, A.S., Balan, K., Javed, Y. Abdullah., J. & Tarmizi, S. (2019). Secure trust-based blockchain architecture to prevent attacks in VANET. Sensors (Switzerland), 19(22), 1.

Khan, A. S., Javed, Y., & Abdullah, J. (2021). Trust-based lightweight security protocol for device to device multihop cellular communication (TLwS). Journal of Ambient Intelligence and Humanized Computing, 10.1007/s12652-021-02968-6.

Khan, A. S., Javed, Y., Saqib, R., Ahmad, Z., Abdullah, J., Zen, K. & Khan, N. (2022). Lightweight Multifactor Authentication Scheme for NextGen Cellular Networks. IEEE Access. 10, 31273–31288.

Khan, A.S., Yahya, M. I., Zen, K., Abdullah, J., Rashid, R. A., Javed, J., Khan, N. A., & Mostafa, A. M "Blockchain-Based Lightweight Multifactor Authentication for Cell-Free in Ultra-Dense 6G-Based (6-CMAS) Cellular Network," in IEEE Access, doi: 10.1109/ACCESS.2023.3249969.

Kilic, S. & Ozkan, O. (2019, July). A self-adaptive UAV routing for forest fire risk mitigation: a conceptual model. In Proceedings of the 2019 Summer Simulation Conference, pp. 1-12.

Li, Y., & Pu, C. (2020, December). Lightweight digital signature solution to defend micro aerial vehicles against man-in-the-middle attack. In 2020 IEEE 23rd international conference on computational science and engineering (CSE), (pp. 92-97.

Liu, Y., Dai, H. N., Wang, Q., Shukla, M. K., & Imran, M. (2020). Unmanned aerial vehicle for internet of everything: Opportunities and challenges. Computer communications, 155, 66-83.

Lopez, M. A., Baddeley, M., Lunardi, W.T., Pandey, A., & Giacalone, J-P. (2021). "Towards Secure Wireless Mesh Networks for UAV Swarm Connectivity: Current Threats, Research, and Opportunities. 17th International Conference in Distributed Computing in Sensor Systems (DCOSS), pp 319-326.

Maikol, S. O., Khan, A. S., Javed, Y., Bunsu, A. L., Petrus, C., George, H., & Jau, S. (2020). A novel authentication and key agreement scheme for countering MITM and impersonation attack in medical facilities. International Journal of Integrated Engineering, vol. 13, no. 2.

Mohammad. Y., Alzahrani, N., Khan, L., Georgieva, A. M., Bamahdi, O. A., & Abdulkader, A. H. (2023). Protecting Attacks on Unmanned Aerial Vehicles using Homomorphic Encryption, Indonesian Journal of Electrical Engineering and Informatics, Vol. 11, No. 1.

Mohsan, S. A. H., Khan, M. A., Noor, F., Ullah, I., & Alsharif, M. H. (2022). Towards the Unmanned Aerial Vehicles (UAVs). A Comprehensive Review. Drones, 6(6), 147.

Raj, J. S. (2021). Security enhanced blockchain based unmanned aerial vehicle health monitoring system. Journal of ISMAC, 3(02), 121-131.

Sekander, S., Tabassum, H., & Hossain, E. (2018). Multi-tier drone architecture for 5G/B5G cellular networks: Challenges, trends, and prospects. IEEE Communications Magazine, 56(3), 96-103.

Shamsoshoara, A., Afghah, F., Razi, A., Mousavi, S., Ashdown, J., & Turk, K. (2020). An autonomous spectrum management scheme for unmanned aerial vehicle networks in disaster relief operations. IEEE Access, 8, 58064-58079.

Su, J., Yu, S., Li, B., & Ye, Y. (2022). "Distributed and Collective Intelligence for Computation Offloading in Aerial Edge Networks. IEEE Transactions on Intelligent Transportation Systems, doi: 10.1109/TITS.2022.3160594.

Torianyk, V. K. (2021, March). IMECA Based Assessment of Internet of Drones Systems Cyber Security Considering Radio Frequency Vulnerabilities. In IntelITSIS, pp. 460-470.

Wang, H. Z. (2019). Survey on unmanned aerial vehicle networks: A cyber physical system perspective. IEEE Communications Surveys & Tutorials, 22(2), 1027-1070.

Zhao, Y., & Smidts, C. (2020). A control-theoretic approach to detecting and distinguishing replay attacks from other anomalies in nuclear power plants. Progress in Nuclear Energy, 123, 103315.

Zhou, Y. R. (2020). UAV swarm intelligence: Recent advances and future trends. IEEE Access, 8, 183856-183878.