PHYSICAL SECURITY DETECTORS FOR CRITICAL INFRASTRUCTURES AGAINST NEW-AGE THREAT OF DRONES AND HUMAN INTRUSION

Xindi Zhang[*], *Krishna Chandramouli*[†], *Dusan Gabrijelcic*[‡], *Theodore Zahariadis*[**], *Gabriele Giunta*[††].

[*]Queen Mary University of London; [†]Venaka Media Limited ;
[‡]Institut Joseph Stefan; [**]University of Athens; [††]ENGINEERING.

ABSTRACT

Modern critical infrastructures are increasingly turning into distributed, complex Cyber-Physical systems that need proactive protection and fast restoration to mitigate physical or cyber incidents or attacks. Addressing the need for early stage threat detection against physical intrusion, the paper presents two physical security sensors developed within the DEFENDER project for detecting the intrusion of drones and humans using video analytics. The continuous stream of media data obtained from the region of vulnerability and proximity is processed using Region based Fully Connected Neural Network deep-learning model. The novelty of the proposed system relies in the processing of multi-threaded media input streams for achieving real-time threat identification. The video analytics solution has been validated using NVIDIA GeForce GTX 1080 for drone detection and NVIDIA GeForce RTX 2070 Max-Q Design for detecting human intruders. The experimental test bed for the validation of the proposed system has been constructed to include environments and situations that are commonly faced by critical infrastructure operators such as the area of protection, tradeoff between angle of coverage against distance of coverage.

Index Terms— Region based Fully Connected Neural Network (RFCN), Intrusion detection, Deep-learning, Critical Infrastructure Security

1. INTRODUCTION

Modern critical infrastructures are increasingly turning into distributed, complex Cyber-Physical systems that need proactive protection and fast restoration to mitigate physical or cyber incidents or attacks, and most importantly combined cyber-physical attacks, which are much more challenging and it is expected to become the most intrusive attack. Addressing the challenges faced by the critical infrastructure operators especially responsible for the production and distribution of energy services, DEFENDER[1] project has developed several cyber-physical detectors and operational blueprints to safeguard the future European Critical Energy Infrastructure (CEI) operation against new and evolving threats. In complementary to the cyber threats, the nature of physical threats is compounded by the use of drones in addition to the human intrusion against the infrastructure with malicious intent. Addressing the threat posed by the physical intrusion, the paper presents the design and validation of two detectors capable of identifying the intruders and signal the command centre of the threat presented. An overview of the design of two detectors is presented in Figure 1. The figure on the left showcases the installation of the drone detector with the use of dual-camera system, which combines the use of region based fully connected neural network (RFCN) [1] with Canny edge detector [2] for drone detection. The detector on the right showcases the installation of the human detector on the fence of the critical infrastructure. The objective of the paper is to outline in detail the operational efficiency of both detectors for detecting the malicious intruders against the infrastructure.

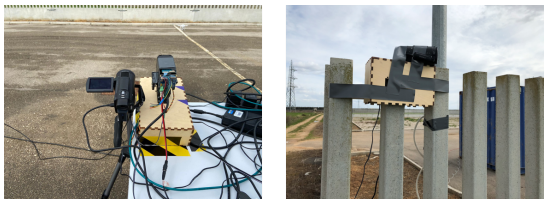

Fig. 1. Detector installation

In the literature there are several examples of deep-learning based intrusion detection. The single-shot object detection model YOLOv2 was used in [3]. Faster R-CNN [4] with two different backbone ZFNet and VGG16 was investigated in [5]. A drone detection and tracking framework was proposed in [6] and the detection part used RFCN with ResNet101. In [7] an artificial images dataset was generated and trained by Faster R-CNN with ResNet101 to address sparse datasets. The computer vision based detector provides accurate determination of intruder objects (both drones and humans) thus enhancing the security protocols of the critical infrastructure operator. The rest of the paper is structured as follows. In Section 2, an overview of the proposed drone detector is presented. In the Section 3, an outline of the human intruder detection is presented based on the video analytics.

[1]https://defender-project.eu/

978-1-7281-1485-9/20/$31.00

Finally, Section 4, summarises the performance evaluation of both detectors on detecting malicious intruders. The paper summaries the findings and lays out a roadmap for the future research direction in Section 6.

2. DRONE INTRUSION DETECTOR

The development in the field of Unmanned Aerial Vehicles (UAV) applications offer possible civil and public domain applications in which single or multiple UAVs may be used. At the same time, it is also critical to realise the potential of misuse by malicious agents and the impact it can have on economic activities. The magnitude of such threats only compounds when the attack is carried out against critical infrastructure. Addressing the need for an early detection system, the functional specification of the drone detector considers two operational states (i) sense objects at the horizon and (ii) detect and recognise the object for deploying countermeasures. To achieve this objective, the system implementation contains four components, namely (i) situation awareness module, (ii) Pan-Tilt-Zoom (PTZ) platform, (iii) multi-class drone classifier using deep-learning, and (iv) alert command center as presented in Figure 2. At beginning, there are two camera, a static camera and a PTZ camera, streaming their video to the system and being aligned at first. The situation awareness module is operate based on the static camera videos to monitor intruders. The PTZ platform consist of a pan-tilt platform with the camera that supports programmatic control of the focal length of the lens. The PTZ signals are processed by the Raspberry Pi for activating the appropriate binary bits interfaced with the servo motors for accurately positioning the platform. The continuous media stream captured by the PTZ camera is transmitted to the analytic component, where the media is processed using the deep-learning network framework for detecting drone and subsequently identify the intruders at the horizon. If the intruder is detected as a drone, the command center will post the situation of the detection and the intrusion evidence. The installation process involves the setup of the detector at the perimeter of the infrastructure. The next step is to configure the operational environment of the detector, which includes the identification of region of attack against the background by aligning both static and PTZ cameras. Subsequently two operating states have been considered by the analytics component and a third state for signalling Raspberry Pi with PTZ instructions.

As the objective of the detector is to provide security for the maximum field of view, the focal length of the static camera is maintained at a minimum. Therefore, the amount of pixel variations captured by the camera is limited to a small region in the image, with effectively few pixel changes. With such a level of low quantity of information available, the deep-learning networks are not able to successfully process the video resulting in the detection. Therefore, the proposed system uses one of the classical vision based techniques for

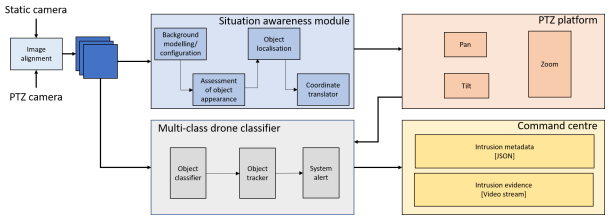

Fig. 2. Building blocks of the drone detector

edge detection namely Canny algorithm [2] to identify the potential objects appearing on the horizon. The operation of the algorithm is summarised in Equation 1, which uses a Gaussian filter to smooth the image and remove noise.

$$H_{ij} = \frac{1}{2\pi\sigma^2} exp\left(-\frac{(i-(k+1))^2 + (j-(k+1))^2}{2\sigma^2}\right); \quad (1)$$

$$1 \leq i, j \leq (2k+1). \quad (2)$$

The equation corresponds to a $(2k+1) \times (2k+1)$ Gaussian filter kernel. The kernel is convoluted with the image to remove high-frequency variations. Subsequently, the image is processed with a Sobel kernel across both vertical and horizontal directions. The derivative in vertical direction (G_y) and horizontal direction (G_x) results in the determination of the edge gradient for each pixels:

$$EdgeGradient(G) = \sqrt{G_x^2 + G_y^2} \quad (3)$$

$$Angle(\theta) = tan^{-1}(\frac{G_y}{G_x}) \quad (4)$$

Following the intensity gradient assigned for each pixel, a threshold is applied above which the pixels are treated as containing an edge, while the pixels below the threshold are ignored. The rest of those will be decided depends on their connectivity. It is important to choose appropriate threshold for better edge result. After getting the edge, the dilation is operated by Equation 5. The maximizing operation enlarge the edges to be an entire foreground.

$$dst(x,y) = \max_{(x',y'):element(x',y')\neq 0} src(x+x', y+y') \quad (5)$$

The bounding box is generated by finding contour of the foreground. The outcome is presented in Figure 3. The localisation of the intruder object to a specific grid in the image captured with the minimal focal length facilitates the analytics component to single the Raspberry Pi and the camera to gather additional information from the respective grid through the pan-tile and zoom operation. The implementation of the drone detection process includes the use of RFCN deep-learning network [1]. The architecture of RFCN is divided into three sub-network: (1) feature extraction, (2) region proposal generation and (3) final classification and bounding box

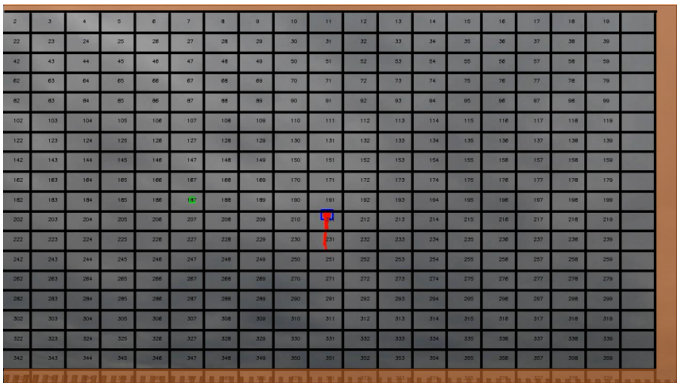

Fig. 3. Intruder object localisation using the edge detection and dilation algorithm

regression. The feature extractor helps to learn the appearance feature of the whole image. The method used is ResNet 101 which has been pre-trained on ImageNet database [8]. An example of the detection outcome is presented in Figure 4. A detailed description of the drone detection is presented in [6].

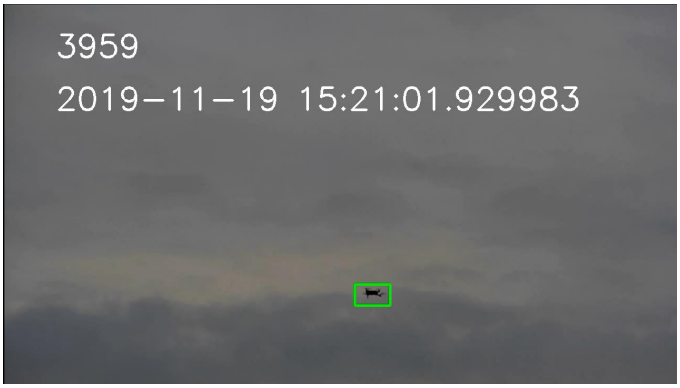

Fig. 4. The result of the drone detection following the PTZ operation using RFCN network

3. HUMAN INTRUSION DETECTION

In addition to the threat posed by the drones, the physical threat posed by humans for gaining unlawful entry into the critical infrastructure also presents an imminent danger. Addressing the challenge of gaining situational awareness in the proximity of the infrastructure, DEFENDER security framework integrates the RFCN deep-learning network based on the ResNet101 feature extractor [1]. The situational awareness component is modelled to translate the geo-location of the malicious intruder in the proximity of the infrastructure perimeter to generate events for which appropriate countermeasures can be deployed in time. An instance of the example of intruder detection against the infrastructure fence is presented in Figure 5.

Fig. 5. Results of intruder detection

method	max distance (m)	ratio
motion detection	80	58
Canny (30,100)	160	116
Canny + sharpen	200	146
Canny (15,300) + sharpen	220	160

Table 1. The capability regards to the method.

4. EXPERIMENTAL RESULT

The evaluation of the proposed system is presented against two key metrics, the long-range distance against which the PTZ operation is triggered followed by the performance of the drone detector implemented using RFCN network. The attack against the infrastructure was simulated using DJI Phantom 3 drone which belongs to the class of mini-drones. The evaluation of the distance at which the objects appearing in the horizon are summarised in Table 1. The evaluation of the proposed approach is presented against the maximum distance at which the ratio of the suspicious object is computed against the overall frame size. The proposed system is able to detect the appearance of malicious drone object at 220 meters in the line of sight of the detector.

4.1. Drone detection accuracy

The evaluation protocols used for drone detection is Average Precision (AP) [9] which is the summary of the shape of the precision/recall curve. The experimental results were carried out on a set of video footage captured in the urban environment with DJI Phantom 3 Standard piloted from the point of attack. A total of 39 attack simulations were created with each attack ranging between 6 to 117 seconds resulting in a cumulative of 12.36 minutes of drone flights. The proposed RFCN Resnet101 network performance has been compared against three other deep-learning network models, namely SSD Mobilenet [10], SSD Inception v2 [11] and Faster RCNN Resnet101 [4]. The result comparison is shown in Table 2.

method	AP
SSD Mobilenet [12, 10]	30.39%
SSD Inception v2 [11]	7.78%
Faster RCNN Resnet101 [4]	69.49%
RFCN Resnet101	81.16%

Table 2. Drone detection accuracy.

4.2. Human intrusion detection accuracy

The operational efficiency of the human intruder detection is presented in 5. The evaluation of the system performance included the computational latency required for the detector to send notifications to the command centre on the appearance of intruders and the evolution of the threats sequence in time. To facilitate the deployment of the countermeasures against the threat the alert sent to the command centre based on the event are separated by 20 seconds. Based on the evolution of the threat, from the proximity of the infrastructure to the approach of the perimeter, the status flag embedded within the alerts are changed from LOW, MEDIUM, HIGH and VERY_HIGH. The experimental evaluation of the detector carried out in the DEFENDER field trail, yielded an accuracy of 96.7% in the person detection.

5. ACKNOWLEDGEMENT

The research work leading to the publication was supported by European Union's Horizon 2020 research and innovation programme under grant agreement no. 740898 - DEFENDER project

6. CONCLUSION

In this paper, the operational prototype of two physical sensors for the detection of intruder drones and human have been presented. The novelty of the drone detector lies in the ability to detect objects appearing on the horizon using the static camera and classify the objects using video data obtained from the PTZ camera. The programmatic control of the focal length of PTZ camera is calculated from the position of drone estimated from the static camera. The signalling of the PTZ platform also leads to the compensation of 3-degrees of freedom in which the malicious drone is piloted. The human intrusion detector is able to generate situational awareness from the person detection model. The future work will continue to investigate approaches to compute the distance which can be used to deploy mitigating strategies for the infrastructure security.

7. REFERENCES

[1] Jifeng Dai, Yi Li, Kaiming He, and Jian Sun, "R-FCN: object detection via region-based fully convolutional networks," *CoRR*, vol. abs/1605.06409, 2016.

[2] J. Canny, "A computational approach to edge detection," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. PAMI-8, no. 6, pp. 679–698, Nov 1986.

[3] C. Aker and S. Kalkan, "Using deep networks for drone detection," in *2017 14th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS)*, Aug 2017, pp. 1–6.

[4] Shaoqing Ren, Kaiming He, Ross B. Girshick, and Jian Sun, "Faster R-CNN: towards real-time object detection with region proposal networks," *CoRR*, vol. abs/1506.01497, 2015.

[5] M. Saqib, S. Daud Khan, N. Sharma, and M. Blumenstein, "A study on detecting drones using deep convolutional neural networks," in *2017 14th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS)*, Aug 2017, pp. 1–5.

[6] Xindi Zhang and Krishna Chandramouli, "Critical infrastructure security against drone attacks using visual analytics," in *Computer Vision Systems*, Dimitrios Tzovaras, Dimitrios Giakoumis, Markus Vincze, and Antonis Argyros, Eds., Cham, 2019, pp. 713–722, Springer International Publishing.

[7] Junkai Peng, Changwen Zheng, Pin Lv, Tianyu Cui, Ye Cheng, and Si Lingyu, "Using images rendered by pbrt to train faster r-cnn for uav detection," 2018.

[8] Olga Russakovsky, Jia Deng, Hao Su, Jonathan Krause, Sanjeev Satheesh, Sean Ma, Zhiheng Huang, Andrej Karpathy, Aditya Khosla, Michael S. Bernstein, Alexander C. Berg, and Fei-Fei Li, "Imagenet large scale visual recognition challenge," *CoRR*, vol. abs/1409.0575, 2014.

[9] Mark Everingham, Luc Van Gool, Christopher K. I. Williams, John Winn, and Andrew Zisserman, "The pascal visual object classes (voc) challenge," *International Journal of Computer Vision*, vol. 88, no. 2, pp. 303–338, Jun 2010.

[10] Wei Liu, Dragomir Anguelov, Dumitru Erhan, Christian Szegedy, Scott E. Reed, Cheng-Yang Fu, and Alexander C. Berg, "SSD: single shot multibox detector," *CoRR*, vol. abs/1512.02325, 2015.

[11] Christian Szegedy, Vincent Vanhoucke, Sergey Ioffe, Jonathon Shlens, and Zbigniew Wojna, "Rethinking the inception architecture for computer vision," *CoRR*, vol. abs/1512.00567, 2015.

[12] Andrew G. Howard, Menglong Zhu, Bo Chen, Dmitry Kalenichenko, Weijun Wang, Tobias Weyand, Marco Andreetto, and Hartwig Adam, "Mobilenets: Efficient convolutional neural networks for mobile vision applications," *CoRR*, vol. abs/1704.04861, 2017.