Abstract

Abstract—Some countries have designed anti-drone systems i.e., detecting, jamming, and camera units. It is a multidis- ciplinary experienced system particularly designed to protect regions and people from cyber-terrorist and oppose unauthorized drones. Security and surveillance are two of the leading areas in the growing drone sector. Moreover, machine learning or deep learning could help in object detection because of its high accuracy and acceptable delay performance. Hence, this paper proposed a modified streaming protocol for drone surveillance with post-quantum cryptography that ensures the drone's data confidentiality. This paper also provided a deep learning receiver to perform object detection by using YOLOv2-Tiny, YOLOv3- Tiny, and YOLOv4-Tiny respectively. The 72 experiment results showed that all configurations on the 30-FPS input produced big overhead and huge delay. This leaves the option to set the FPS input to be lower than 30, yet the FPS benchmark result showed that even with the highest FPS configuration, the results were capped at a maximum of 14-FPS. Nevertheless, the results of the proposed methods confirmed the feasibility of using the developed surveillance drone on low-energy architecture. **Index Terms—drone, post-quantum, shor algorithm, internet of things, surveillance**