125
ENG

Predicting and Mitigating Cyber Threats on Urban Air Mobility Through Reinforcement Learning

Abstract

The Urban Air Mobility (UAM) market is undergoing exponential growth with applications ranging from security, drones, to air taxis. However, this growth introduces a vulnerability. The connectivity of UAM's to public network infrastructure makes them susceptible to malicious cyberattacks, with the latest and most common ones being de-authentication, Denial of Service (DoS), and UDP Flood attacks. These attacks pose a threat to the proper functionality of UAM and incur significant costs to remedy. Researchers have responded by developing models to predict these modern cyberattacks, primarily relying on computationally heavy supervised learning algorithms. Despite their high success rate, these algorithms are impractical for UAM use. A potential solution lies in transitioning to reinforcement learning. Reinforced learning is a computationally lighter alternative that suits UAM's operational requirements. Furthermore, it requires less data for training while maintaining accuracy in predicting cyberattacks. This study focuses on the Parrot AR.Drone 2.0, a specific yet widely adopted Urban Air Mobility device, due to affordability. The primary objective of this research is to utilize reinforcement learning in predicting de-authentication, Denial-of-Service (DoS), and UDP Flood attacks on the drone. The model's outcomes demonstrate a predictive accuracy of the above listed cyberattacks of 95.5% using reinforced learning algorithm. Although this accuracy rating falls short of its supervised learning algorithm counterparts, reinforcement learning still maintains the advantage of demanding less data to train while lightening the computational burden on UAM systems.