Zero Trust-based Collaborative Drone System with Intelligence-driven Edge Routing

With the ability to extend the capabilities of cloud computing, mobile edge computing has become increasingly utilized. In numerous cases, edge routing mechanisms can be used with mobile ad hoc networks (MANETs) to manage data network transmission in areas where conventional networks would fail. Securing these networks is challenging due to their stateless nature and resource constrained devices. In addition, MANETs pose challenges that traditional security frameworks are not designed to meet. The Zero Trust (ZT) paradigm can solve these issues by offering adaptable defense strategies. A ZT approach can take static or network-based perimeter security that is found in traditional networks and shift the focus on users, assets, and resources, providing superior security mechanisms to these systems.

In this paper, we propose a novel ZT security framework for intelligence-driven edge routing for a collaborative drone system application. We model threats that focus on preventing and mitigating common attacks that occur within the packet and network-level of collaborative drone systems. Because of the resource constraints present in these systems, we implement our ZT framework with an emphasis on low overhead for resource-constrained devices with a novel architecture for offloading resource-dependent security tasks. This is accomplished by offloading the large computational tasks to an additional Ground Control Station (GCS) at the edge of the network that has the burden of trust management.

We evaluate the efficiency and effectiveness of our ZT approach through simulations in the open-source network simulator (NS-3) in an extendable, and reproducible manner on different edge routing approaches. The experimental results indicate the effectiveness of our system, detecting and mitigating threats at the packet and network levels on resource and energy constrained drone systems.