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. In addition, securing these networks, composed of resource-constrained devices and stateless networks, poses challenges that traditional security frameworks are not designed to meet. The Zero Trust (ZT) approach is a paradigm that can solve these issues and be adaptable, evolving defense strategies of static, or network-based perimeters and focus on users, assets, and resources, being an excellent approach to provide 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, modeling threats that focuses 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. Packet and network-level attacks are considered, and the ZT approach is compared with traditional security schemes. 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 in a hybrid testbed implementation composed of the open-source network simulator (NS-3) and a platform for wireless networks (POWDER), making it realistic, extendable, and reproducible. The experimental results indicate the effectiveness of our system, detecting and mitigating threats in packet and network levels on resource constrained drone systems.